# Scan Report

February 12, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Webmail de l'Université". The scan started at Wed Feb 12 11:36:43 2025 UTC and ended at Wed Feb 12 13:24:25 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 172.20.1.252<br>webmail.univ-lome.tg | 0 | 8 | 1 | 0 | 0 |
| Total: 1 | 0 | 8 | 1 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 9 results selected by the filtering described above. Before filtering there were 180 results.

# 2 Results per Host

## 2.1 172.20.1.252

| | |
|---|---|
| Host scan start | Wed Feb 12 11:37:37 2025 UTC |
| Host scan end | Wed Feb 12 13:24:18 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 25/tcp | Medium |
| 8443/tcp | Medium |
| 587/tcp | Medium |
| 110/tcp | Medium |
| 143/tcp | Medium |
| 465/tcp | Medium |
| 22/tcp | Low |

### 2.1.1 Medium 25/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

**Summary**

. . . continues on next page . . .

... continued from previous page ...

The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**

```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪----------------------------------------------
TLSv1.2          | 10
```

**Impact**

The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

**Solution:**

**Solution type:** VendorFix

Users should contact their vendors for specific patch information.

A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

**Affected Software/OS**

Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

**Vulnerability Insight**

The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.

Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:

> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.

Both CVEs are still kept in this VT as a reference to the origin of this flaw.

**Vulnerability Detection Method**

Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.

Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`

OID:1.3.6.1.4.1.25623.1.0.117761

Version used: `2024-09-27T05:05:23Z`

**References**

```
cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego
↪tiation-dos/
```

... continues on next page ...

... continued from previous page ...

```
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
url: https://www.openwall.com/lists/oss-security/2011/07/08/2
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-0796
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K17/0980
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112
```

[ return to 172.20.1.252 ]

### 2.1.2 Medium 8443/tcp

Medium (CVSS: 5.0)
NVT: Backup File Scanner (HTTP) - Reliable Detection Reporting

**Summary**
The script reports backup files left on the web server.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The following backup files were identified (<URL>:<Matching pattern>):`
`https://webmail.univ-lome.tg:8443/config/config.inc.php.orig:^<\?(php|=)`

**Impact**
Based on the information provided in these files an attacker might be able to gather sensitive information stored in these files.

**Solution:**
**Solution type:** Mitigation
Delete the backup files.

**Vulnerability Insight**
Notes:
- 'Reliable Detection' means that a file was detected based on a strict (regex) and reliable pattern matching the response of the remote web server when a file was requested.

... continues on next page ...

... continued from previous page ...

- As the VT 'Backup File Scanner (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.140853) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

**Vulnerability Detection Method**
Reports previous enumerated backup files accessible on the remote web server.
Details: `Backup File Scanner (HTTP) - Reliable Detection Reporting`
OID:1.3.6.1.4.1.25623.1.0.108976
Version used: `2022-09-13T10:15:09Z`

**References**
`url: http://www.openwall.com/lists/oss-security/2017/10/31/1`

[ return to 172.20.1.252 ]

### 2.1.3 Medium 587/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)`

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
`'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:`
`TLS_RSA_WITH_SEED_CBC_SHA`

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:

... continues on next page ...

... continued from previous page ...

- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

**Summary**
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**

```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪-------------------------------------------------
TLSv1.2          | 10
```

**Impact**
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

**Affected Software/OS**
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

**Vulnerability Insight**
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

**Vulnerability Detection Method**
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: `2024-09-27T05:05:23Z`

**References**
`cve: CVE-2011-1473`
`cve: CVE-2011-5094`
`url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego`
`↪tiation-dos/`
`url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/`
`url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation`
`url: https://www.openwall.com/lists/oss-security/2011/07/08/2`
`cert-bund: WID-SEC-2024-1591`
`cert-bund: WID-SEC-2024-0796`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K17/0980`
`cert-bund: CB-K17/0979`
`cert-bund: CB-K14/0772`
`cert-bund: CB-K13/0915`
`cert-bund: CB-K13/0462`
`dfn-cert: DFN-CERT-2017-1013`
`dfn-cert: DFN-CERT-2017-1012`
`dfn-cert: DFN-CERT-2014-0809`
`dfn-cert: DFN-CERT-2013-1928`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2012-1112

[ return to 172.20.1.252 ]

### 2.1.4 Medium 110/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

**Summary**
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**

```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪------------------------------------------------
TLSv1.2          | 10
```

**Impact**
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

**Solution:**
**Solution type:** VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

**Affected Software/OS**
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

**Vulnerability Insight**
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

**Vulnerability Detection Method**

... continues on next page ...

... continued from previous page ...

Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: 2024-09-27T05:05:23Z

**References**

cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego
↪tiation-dos/
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
url: https://www.openwall.com/lists/oss-security/2011/07/08/2
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-0796
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K17/0980
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112

[ return to 172.20.1.252 ]

### 2.1.5 Medium 143/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

**Summary**

The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**

```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪-------------------------------------------------
```

... continues on next page ...

... continued from previous page ...

| | |
|---|---|
| TLSv1.2 | 10 |

**Impact**
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

**Solution:**
**Solution type:** VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

**Affected Software/OS**
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

**Vulnerability Insight**
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

**Vulnerability Detection Method**
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: 2024-09-27T05:05:23Z

**References**
cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego
↪tiation-dos/
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
url: https://www.openwall.com/lists/oss-security/2011/07/08/2
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-0796
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K17/0980
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112
```

[ return to 172.20.1.252 ]

### 2.1.6 Medium 465/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_SEED_CBC_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium

... continues on next page ...

... continued from previous page ...

- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977

Medium (CVSS: 5.4)
NVT: SSL/TLS: Report 'Anonymous' Cipher Suites

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all 'Anonymous' SSL/TLS cipher suites accepted by a service.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA256
TLS_DH_anon_WITH_AES_128_GCM_SHA256
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA256
TLS_DH_anon_WITH_AES_256_GCM_SHA384
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA

... continues on next page ...

... continued from previous page ...

TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA

**Impact**
This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed 'Anonymous' cipher suites anymore.
Please see the references for more resources supporting you in this task.

**Vulnerability Insight**
Services supporting 'Anonymous' cipher suites could allow a client to negotiate an SSL/TLS connection to the host without any authentication of the remote endpoint.

**Vulnerability Detection Method**
Details: SSL/TLS: Report 'Anonymous' Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.108147
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2007-1858
cve: CVE-2014-0351
url: https://bettercrypto.org/
url: http://www.securityfocus.com/bid/28482
url: http://www.securityfocus.com/bid/69754
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K14/0058
dfn-cert: DFN-CERT-2014-0049
dfn-cert: DFN-CERT-2012-0442

[ return to 172.20.1.252 ]

### 2.1.7 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm(s):
umac-64-etm@openssh.com
umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**

. . . continues on next page . . .

... continued from previous page ...

```
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4
```

[ return to 172.20.1.252 ]

---

# Scan Report

February 14, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "SRV_UL". The scan started at Thu Feb 13 07:22:00 2025 UTC and ended at Thu Feb 13 19:37:45 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 172.20.1.11 | 2 | 6 | 1 | 0 | 0 |
| 172.20.1.23 | 2 | 5 | 1 | 0 | 0 |
| 172.20.1.8 | 1 | 3 | 1 | 0 | 0 |
| 172.20.1.58 | 1 | 6 | 1 | 0 | 0 |
| 172.20.1.18 | 1 | 3 | 1 | 0 | 0 |
| 172.20.1.2 | 1 | 4 | 1 | 0 | 0 |
| 172.20.1.201 | 0 | 9 | 1 | 0 | 0 |
| 172.20.1.250 | 0 | 2 | 1 | 0 | 0 |
| 172.20.1.71 | 0 | 3 | 1 | 0 | 0 |
| 172.20.1.252 | 0 | 8 | 1 | 0 | 0 |
| 172.20.1.3 | 0 | 2 | 0 | 0 | 0 |
| 172.20.1.60 | 0 | 4 | 1 | 0 | 0 |
| 172.20.1.6 | 0 | 1 | 1 | 0 | 0 |
| 172.20.1.21 | 0 | 1 | 1 | 0 | 0 |
| 172.20.1.24<br>univ-lome.tg | 0 | 2 | 1 | 0 | 0 |
| 172.20.1.9 | 0 | 2 | 1 | 0 | 0 |
| 172.20.1.55 | 0 | 2 | 1 | 0 | 0 |
| 172.20.1.57 | 0 | 1 | 0 | 0 | 0 |
| 172.20.1.4 | 0 | 5 | 1 | 0 | 0 |
| 172.20.1.253 | 0 | 1 | 0 | 0 | 0 |
| 172.20.1.35 | 0 | 0 | 1 | 0 | 0 |
| 172.20.1.160 | 0 | 0 | 1 | 0 | 0 |
| 172.20.1.56 | 0 | 0 | 1 | 0 | 0 |
| 172.20.1.10 | 0 | 0 | 1 | 0 | 0 |
| 172.20.1.41 | 0 | 0 | 1 | 0 | 0 |
| 172.20.1.42 | 0 | 0 | 1 | 0 | 0 |
| 172.20.1.14 | 0 | 0 | 1 | 0 | 0 |
| 172.20.1.15 | 0 | 0 | 1 | 0 | 0 |
| 172.20.1.7 | 0 | 0 | 1 | 0 | 0 |
| 172.20.1.153 | 0 | 0 | 1 | 0 | 0 |
| Total: 30 | 8 | 70 | 27 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level “Log” are not shown.
Issues with the threat level “Debug” are not shown.
Issues with the threat level “False Positive” are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 105 results selected by the filtering described above. Before filtering there were 2538 results.

# 2 Results per Host

## 2.1 172.20.1.11

| | |
|---|---|
| Host scan start | Thu Feb 13 14:24:19 2025 UTC |
| Host scan end | Thu Feb 13 15:40:00 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| general/tcp | High |
| 443/tcp | High |
| 22/tcp | Medium |
| 443/tcp | Medium |
| 22/tcp | Low |

### 2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: Operating System (OS) End of Life (EOL) Detection

**Product detection result**
cpe:/o:centos:centos:7
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)

**Summary**
The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The "CentOS" Operating System on the remote host has reached the end of life.
CPE: cpe:/o:centos:centos:7
Installed version,
build or SP: 7
EOL date: 2024-06-30
EOL info: http://wiki.centos.org/Download

**Impact**

. . . continues on next page . . .

... continued from previous page ...

An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

**Solution:**
**Solution type:** Mitigation
Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

**Vulnerability Detection Method**
Checks if an EOL version of an OS is present on the target host.
Details: `Operating System (OS) End of Life (EOL) Detection`
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: `2024-02-28T14:37:42Z`

**Product Detection Result**
Product: `cpe:/o:centos:centos:7`
Method: `OS Detection Consolidation and Reporting`
OID: 1.3.6.1.4.1.25623.1.0.105937)

[ return to 172.20.1.11 ]

### 2.1.2 High 443/tcp

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.`
`↪802067)`

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```

... continues on next page ...

... continued from previous page ...

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 172.20.1.11 ]

### 2.1.3 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Product detection result**

```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

**Summary**

The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                      | Reason
-----------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

**Impact**

An attacker can quickly break individual connections.

**Solution:**

**Solution type:** Mitigation

Disable the reported weak KEX algorithm(s)

- 1024-bit MODP group / prime KEX algorithms:

Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

**Vulnerability Insight**

- 1024-bit MODP group / prime KEX algorithms:

Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.

... continues on next page ...

... continued from previous page ...

A nation-state can break a 1024-bit prime.

**Vulnerability Detection Method**
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://weakdh.org/sysadmin.html`
`url: https://www.rfc-editor.org/rfc/rfc9142`
`url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem`
`url: https://www.rfc-editor.org/rfc/rfc6194`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5`

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565`
`↪)`

**Summary**
The remote SSH server is configured to allow / support weak encryption algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The remote SSH server supports the following weak client-to-server encryption al`
`↪gorithm(s):`
`3des-cbc`
`aes128-cbc`
`aes192-cbc`
`aes256-cbc`
`blowfish-cbc`

... continues on next page ...

... continued from previous page ...

```
cast128-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
```

**Solution:**
**Solution type:** Mitigation
Disable the reported weak encryption algorithm(s).

**Vulnerability Insight**
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

**Vulnerability Detection Method**
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms
Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc8758`
`url: https://www.kb.cert.org/vuls/id/958563`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3`

[ return to 172.20.1.11 ]

### 2.1.4 Medium 443/tcp

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

**Summary**
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
`The web server has the following HTTP methods enabled: TRACE`

**Impact**
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

**Solution:**
**Solution type:** Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

**Affected Software/OS**
Web servers with enabled TRACE and/or TRACK methods.

**Vulnerability Insight**
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

**Vulnerability Detection Method**
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2023-08-01T13:29:10Z`

**References**
`cve: CVE-2003-1567`
`cve: CVE-2004-2320`
`cve: CVE-2004-2763`
`cve: CVE-2005-3398`
`cve: CVE-2006-4683`
`cve: CVE-2007-3008`
`cve: CVE-2008-7253`
`cve: CVE-2009-2823`
`cve: CVE-2010-0386`
`cve: CVE-2012-2223`

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2014-7883
url: http://www.kb.cert.org/vuls/id/288308
url: http://www.securityfocus.com/bid/11604
url: http://www.securityfocus.com/bid/15222
url: http://www.securityfocus.com/bid/19915
url: http://www.securityfocus.com/bid/24456
url: http://www.securityfocus.com/bid/33374
url: http://www.securityfocus.com/bid/36956
url: http://www.securityfocus.com/bid/36990
url: http://www.securityfocus.com/bid/37995
url: http://www.securityfocus.com/bid/9506
url: http://www.securityfocus.com/bid/9561
url: http://www.kb.cert.org/vuls/id/867593
url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac
↪e-verbs/ba-p/784482
url: https://owasp.org/www-community/attacks/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

**Summary**

The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
The certificate of the remote service expired on 2021-09-24 08:08:59.
Certificate details:
fingerprint (SHA-1)                | 869C422E3E7041FEB179F58F5345A248D427D9BB
fingerprint (SHA-256)              | 8F24A9D6368AB8F7DDE36E3A18A9F5DBD55AFD24B62E81
↪1A9BB6C90C470C66AE
issued by                          | 1.2.840.113549.1.9.1=#726F6F74406C6F63616C686F
↪73742E6C6F63616C646F6D61696E,CN=localhost.localdomain,OU=SomeOrganizationalUni
↪t,O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
public key algorithm               | RSA
public key size (bits)             | 2048
```

... continues on next page ...

... continued from previous page ...

| | |
|---|---|
| serial | 008C |
| signature algorithm | sha256WithRSAEncryption |
| subject | 1.2.840.113549.1.9.1=#726F6F74406C6F63616C686F73742E6C6F63616C646F6D61696E,CN=localhost.localdomain,OU=SomeOrganizationalUnit,O=SomeOrganization,L=SomeCity,ST=SomeState,C=-- |
| subject alternative names (SAN) | None |
| valid from | 2020-09-24 08:08:59 UTC |
| valid until | 2021-09-24 08:08:59 UTC |

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 5.0)
NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25623.1.0.103692)

**Summary**
The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
The certificate of the remote service is signed by the following untrusted and/or dangerous CA:

... continues on next page ...

... continued from previous page ...

```
Issuer: 1.2.840.113549.1.9.1=#726F6F74406C6F63616C686F73742E6C6F63616C646F6D6169
↪6E,CN=localhost.localdomain,OU=SomeOrganizationalUnit,O=SomeOrganization,L=Som
↪eCity,ST=SomeState,C=--
Certificate details:
fingerprint (SHA-1)              | 869C422E3E7041FEB179F58F5345A248D427D9BB
fingerprint (SHA-256)            | 8F24A9D6368AB8F7DDE36E3A18A9F5DBD55AFD24B62E81
↪1A9BB6C90C470C66AE
issued by                        | 1.2.840.113549.1.9.1=#726F6F74406C6F63616C686F
↪73742E6C6F63616C646F6D61696E,CN=localhost.localdomain,OU=SomeOrganizationalUni
↪t,O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
public key algorithm             | RSA
public key size (bits)           | 2048
serial                           | 008C
signature algorithm              | sha256WithRSAEncryption
subject                          | 1.2.840.113549.1.9.1=#726F6F74406C6F63616C686F
↪73742E6C6F63616C646F6D61696E,CN=localhost.localdomain,OU=SomeOrganizationalUni
↪t,O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
subject alternative names (SAN)  | None
valid from                       | 2020-09-24 08:08:59 UTC
valid until                      | 2021-09-24 08:08:59 UTC
```

**Impact**
An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate with one signed by a trusted CA.

**Vulnerability Detection Method**
The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.
Details: `SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection`
OID:1.3.6.1.4.1.25623.1.0.113054
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**
`cpe:/a:ietf:transport_layer_security:1.0`

... continues on next page ...

... continued from previous page ...

Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security:1.0
Method: SSL/TLS: Version Detection

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**

cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

[ return to 172.20.1.11 ]

### 2.1.5 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**

```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

**Summary**

The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
```

... continues on next page ...

... continued from previous page ...

umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[ return to 172.20.1.11 ]

## 2.2 172.20.1.23

Host scan start Thu Feb 13 13:09:07 2025 UTC
Host scan end Thu Feb 13 14:42:55 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | High |
| general/tcp | High |
| 22/tcp | Medium |
| 443/tcp | Medium |
| 22/tcp | Low |

### 2.2.1 High 443/tcp

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
. . . continues on next page . . .

... continued from previous page ...

Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 172.20.1.23 ]

### 2.2.2 High general/tcp

High (CVSS: 10.0)
NVT: Operating System (OS) End of Life (EOL) Detection

**Product detection result**
cpe:/o:centos:centos:7
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)

**Summary**
The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

**Quality of Detection (QoD):** 80%

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**
The "CentOS" Operating System on the remote host has reached the end of life.
CPE: cpe:/o:centos:centos:7
Installed version,
build or SP: 7
EOL date: 2024-06-30
EOL info: http://wiki.centos.org/Download

**Impact**
An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

**Solution:**
**Solution type:** Mitigation
Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

**Vulnerability Detection Method**
Checks if an EOL version of an OS is present on the target host.
Details: Operating System (OS) End of Life (EOL) Detection
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: 2024-02-28T14:37:42Z

**Product Detection Result**
Product: cpe:/o:centos:centos:7
Method: OS Detection Consolidation and Reporting
OID: 1.3.6.1.4.1.25623.1.0.105937)

[ return to 172.20.1.23 ]

### 2.2.3 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

... continues on next page ...

... continued from previous page ...

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                     | Reason
----------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

**Impact**

An attacker can quickly break individual connections.

**Solution:**

**Solution type:** Mitigation

Disable the reported weak KEX algorithm(s)

- 1024-bit MODP group / prime KEX algorithms:

Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

**Vulnerability Insight**

- 1024-bit MODP group / prime KEX algorithms:

Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.

A nation-state can break a 1024-bit prime.

**Vulnerability Detection Method**

Checks the supported KEX algorithms of the remote SSH server.

Currently weak KEX algorithms are defined as the following:

- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key

Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`

OID:1.3.6.1.4.1.25623.1.0.150713

Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**

Product: `cpe:/a:ietf:secure_shell_protocol`

Method: `SSH Protocol Algorithms Supported`

OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**

... continues on next page ...

... continued from previous page ...

url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak encryption algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc

**Solution:**
**Solution type:** Mitigation
Disable the reported weak encryption algorithm(s).

**Vulnerability Insight**
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.

... continues on next page ...

... continued from previous page ...

- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

**Vulnerability Detection Method**
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms
Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc8758`
`url: https://www.kb.cert.org/vuls/id/958563`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3`

[ return to 172.20.1.23 ]

### 2.2.4 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Product detection result**
`cpe:/a:ietf:secure_sockets_layer:3.0`
`Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)`

**Summary**
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

... continues on next page ...

... continued from previous page ...

In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

**Vulnerability Detection Method**
Check the used SSL protocols of the services provided by this system.
Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_sockets_layer:3.0
Method: SSL/TLS: Version Detection
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
cve: CVE-2016-0800
cve: CVE-2014-3566
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://drownattack.com/
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2023-0431
cert-bund: WID-SEC-2023-0427
cert-bund: CB-K18/0094
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1141
cert-bund: CB-K16/1107
cert-bund: CB-K16/1102
cert-bund: CB-K16/0792
cert-bund: CB-K16/0599
cert-bund: CB-K16/0597
cert-bund: CB-K16/0459
cert-bund: CB-K16/0456
cert-bund: CB-K16/0433
cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

**Summary**

This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
```

... continues on next page ...

... continued from previous page ...

'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**
`cpe:/a:ietf:secure_sockets_layer:3.0`

... continues on next page ...

... continued from previous page ...

Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_sockets_layer:3.0
Method: SSL/TLS: Version Detection

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**

cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

[ return to 172.20.1.23 ]

### 2.2.5 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**

```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

**Summary**

The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
```

... continues on next page ...

... continued from previous page ...

umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[ return to 172.20.1.23 ]

## 2.3 172.20.1.8

Host scan start Thu Feb 13 09:45:10 2025 UTC
Host scan end Thu Feb 13 10:37:49 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| general/tcp | High |
| 22/tcp | Medium |
| 80/tcp | Medium |
| 22/tcp | Low |

### 2.3.1 High general/tcp

High (CVSS: 10.0)
NVT: Operating System (OS) End of Life (EOL) Detection

**Product detection result**
cpe:/o:centos:centos:7
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)

**Summary**
The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The "CentOS" Operating System on the remote host has reached the end of life.
CPE: cpe:/o:centos:centos:7
Installed version,
build or SP: 7
EOL date: 2024-06-30
EOL info: http://wiki.centos.org/Download

**Impact**
An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

**Solution:**
**Solution type:** Mitigation
Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

**Vulnerability Detection Method**
Checks if an EOL version of an OS is present on the target host.
Details: Operating System (OS) End of Life (EOL) Detection
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: 2024-02-28T14:37:42Z

**Product Detection Result**
Product: cpe:/o:centos:centos:7
Method: OS Detection Consolidation and Reporting
OID: 1.3.6.1.4.1.25623.1.0.105937)

[ return to 172.20.1.8 ]

### 2.3.2 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm | Reason
---
↪----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1 | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1

**Impact**
An attacker can quickly break individual connections.

**Solution:**
**Solution type:** Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

**Vulnerability Insight**
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

**Vulnerability Detection Method**
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

. . . continues on next page . . .

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.150713
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak encryption algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc

... continues on next page ...

... continued from previous page ...

cast128-cbc

**Solution:**
**Solution type:** Mitigation
Disable the reported weak encryption algorithm(s).

**Vulnerability Insight**
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

**Vulnerability Detection Method**
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms
Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc8758`
`url: https://www.kb.cert.org/vuls/id/958563`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3`

[ return to 172.20.1.8 ]

### 2.3.3 Medium 80/tcp

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

**Summary**

... continues on next page ...

... continued from previous page ...

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
`The web server has the following HTTP methods enabled: TRACE`

**Impact**
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

**Solution:**
**Solution type:** Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

**Affected Software/OS**
Web servers with enabled TRACE and/or TRACK methods.

**Vulnerability Insight**
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

**Vulnerability Detection Method**
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2023-08-01T13:29:10Z`

**References**
`cve: CVE-2003-1567`
`cve: CVE-2004-2320`
`cve: CVE-2004-2763`
`cve: CVE-2005-3398`
`cve: CVE-2006-4683`
`cve: CVE-2007-3008`
`cve: CVE-2008-7253`
`cve: CVE-2009-2823`
`cve: CVE-2010-0386`
`cve: CVE-2012-2223`
`cve: CVE-2014-7883`
`url: http://www.kb.cert.org/vuls/id/288308`
`url: http://www.securityfocus.com/bid/11604`
`url: http://www.securityfocus.com/bid/15222`
`url: http://www.securityfocus.com/bid/19915`

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/24456
url: http://www.securityfocus.com/bid/33374
url: http://www.securityfocus.com/bid/36956
url: http://www.securityfocus.com/bid/36990
url: http://www.securityfocus.com/bid/37995
url: http://www.securityfocus.com/bid/9506
url: http://www.securityfocus.com/bid/9561
url: http://www.kb.cert.org/vuls/id/867593
url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac
↪e-verbs/ba-p/784482
url: https://owasp.org/www-community/attacks/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020
```

[ return to 172.20.1.8 ]

### 2.3.4 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**

```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

**Summary**

The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

**Solution:**

... continues on next page ...

... continued from previous page ...

**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[ return to 172.20.1.8 ]

## 2.4 172.20.1.58

Host scan start Thu Feb 13 14:29:52 2025 UTC
Host scan end Thu Feb 13 15:58:12 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| general/tcp | High |
| 22/tcp | Medium |
| 80/tcp | Medium |
| 8080/tcp | Medium |
| 22/tcp | Low |

### 2.4.1 High general/tcp

High (CVSS: 10.0)
NVT: Operating System (OS) End of Life (EOL) Detection

**Product detection result**
cpe:/o:centos:centos:7
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)

**Summary**
The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The "CentOS" Operating System on the remote host has reached the end of life.
CPE: cpe:/o:centos:centos:7
Installed version,
build or SP: 7
EOL date: 2024-06-30
EOL info: http://wiki.centos.org/Download

**Impact**
An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

**Solution:**
**Solution type:** Mitigation
Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

**Vulnerability Detection Method**
Checks if an EOL version of an OS is present on the target host.
Details: Operating System (OS) End of Life (EOL) Detection
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: 2024-02-28T14:37:42Z

**Product Detection Result**
Product: cpe:/o:centos:centos:7
Method: OS Detection Consolidation and Reporting
OID: 1.3.6.1.4.1.25623.1.0.105937)

[ return to 172.20.1.58 ]

### 2.4.2 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                      | Reason
-----------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

**Impact**
An attacker can quickly break individual connections.

**Solution:**
**Solution type:** Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

**Vulnerability Insight**
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

**Vulnerability Detection Method**
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`

. . . continues on next page . . .

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.150713
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak encryption algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc

... continues on next page ...

... continued from previous page ...

cast128-cbc

**Solution:**
**Solution type:** Mitigation
Disable the reported weak encryption algorithm(s).

**Vulnerability Insight**
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

**Vulnerability Detection Method**
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms
Details: Weak Encryption Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc8758
url: https://www.kb.cert.org/vuls/id/958563
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3

[ return to 172.20.1.58 ]

### 2.4.3 Medium 80/tcp

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

**Summary**

... continues on next page ...

... continued from previous page ...

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
`The web server has the following HTTP methods enabled: TRACE`

**Impact**
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

**Solution:**
**Solution type:** Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

**Affected Software/OS**
Web servers with enabled TRACE and/or TRACK methods.

**Vulnerability Insight**
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

**Vulnerability Detection Method**
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2023-08-01T13:29:10Z`

**References**
`cve: CVE-2003-1567`
`cve: CVE-2004-2320`
`cve: CVE-2004-2763`
`cve: CVE-2005-3398`
`cve: CVE-2006-4683`
`cve: CVE-2007-3008`
`cve: CVE-2008-7253`
`cve: CVE-2009-2823`
`cve: CVE-2010-0386`
`cve: CVE-2012-2223`
`cve: CVE-2014-7883`
`url: http://www.kb.cert.org/vuls/id/288308`
`url: http://www.securityfocus.com/bid/11604`
`url: http://www.securityfocus.com/bid/15222`
`url: http://www.securityfocus.com/bid/19915`

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/24456
url: http://www.securityfocus.com/bid/33374
url: http://www.securityfocus.com/bid/36956
url: http://www.securityfocus.com/bid/36990
url: http://www.securityfocus.com/bid/37995
url: http://www.securityfocus.com/bid/9506
url: http://www.securityfocus.com/bid/9561
url: http://www.kb.cert.org/vuls/id/867593
url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac
↪e-verbs/ba-p/784482
url: https://owasp.org/www-community/attacks/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020
```

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The following input fields were identified (URL:input name):`
`http://172.20.1.58/login:_password`

**Impact**
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**

... continues on next page ...

... continued from previous page ...

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

**References**
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[ return to 172.20.1.58 ]

### 2.4.4 Medium 8080/tcp

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

**Summary**
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
`The web server has the following HTTP methods enabled: TRACE`

**Impact**
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

**Solution:**
**Solution type:** Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

**Affected Software/OS**
Web servers with enabled TRACE and/or TRACK methods.

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

**Vulnerability Detection Method**
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2023-08-01T13:29:10Z`

**References**
cve: CVE-2003-1567
cve: CVE-2004-2320
cve: CVE-2004-2763
cve: CVE-2005-3398
cve: CVE-2006-4683
cve: CVE-2007-3008
cve: CVE-2008-7253
cve: CVE-2009-2823
cve: CVE-2010-0386
cve: CVE-2012-2223
cve: CVE-2014-7883
url: http://www.kb.cert.org/vuls/id/288308
url: http://www.securityfocus.com/bid/11604
url: http://www.securityfocus.com/bid/15222
url: http://www.securityfocus.com/bid/19915
url: http://www.securityfocus.com/bid/24456
url: http://www.securityfocus.com/bid/33374
url: http://www.securityfocus.com/bid/36956
url: http://www.securityfocus.com/bid/36990
url: http://www.securityfocus.com/bid/37995
url: http://www.securityfocus.com/bid/9506
url: http://www.securityfocus.com/bid/9561
url: http://www.kb.cert.org/vuls/id/867593
url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac
↪e-verbs/ba-p/784482
url: https://owasp.org/www-community/attacks/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**

... continues on next page ...

... continued from previous page ...

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The following input fields were identified (URL:input name):`
`http://172.20.1.58:8080/login:_password`

**Impact**
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

**References**
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[ return to 172.20.1.58 ]

### 2.4.5 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
. . . continues on next page . . .

... continued from previous page ...

```
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4
```

[ return to 172.20.1.58 ]

## 2.5 172.20.1.18

Host scan start Thu Feb 13 15:56:31 2025 UTC
Host scan end Thu Feb 13 19:37:38 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | High |
| 5693/tcp | Medium |
| 80/tcp | Medium |
| 22/tcp | Low |

### 2.5.1 High 80/tcp

High (CVSS: 9.8)
NVT: PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check

**Summary**
PHP is prone to multiple vulnerabilities.

**Quality of Detection (QoD):** 95%

**Vulnerability Detection Result**

```
By doing the following HTTP POST request:
"HTTP POST" body : <?php phpinfo();?>
URL              : http://172.20.1.18/php/info.php?-d+allow_url_include%3don+-d+
↪auto_prepend_file%3dphp://input
it was possible to execute the "<?php phpinfo();?>" command.
Result:
  <title>PHP 7.4.33 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFO
↪LLOW,NOARCHIVE" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↪p/7.4/apache2 </td></tr>
  <h2>PHP Variables</h2>
```

**Impact**
Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer. Other attacks are also possible.

**Solution:**

... continues on next page ...

... continued from previous page ...

**Solution type:** VendorFix
Update to version 5.3.13, 5.4.3 or later.

**Affected Software/OS**
PHP versions prior to 5.3.13 and 5.4.x prior to 5.4.3.

**Vulnerability Insight**
When PHP is used in a CGI-based setup (such as Apache's mod_cgid), the php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the php-cgi binary, which can be exploited to disclose source code and obtain arbitrary code execution.
An example of the -s command, allowing an attacker to view the source code of index.php is below:
http://example.com/index.php?-s

**Vulnerability Detection Method**
Send multiple a crafted HTTP POST requests and checks the responses.
This script checks for the presence of CVE-2012-1823 which indicates that the system is also vulnerable against the other included CVEs.
Details: `PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check`
OID:1.3.6.1.4.1.25623.1.0.103482
Version used: `2024-11-26T07:35:52Z`

**References**
`cve: CVE-2012-1823`
`cve: CVE-2012-2311`
`cve: CVE-2012-2336`
`cve: CVE-2012-2335`
`url: https://web.archive.org/web/20190212080415/http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/`
`url: https://www.kb.cert.org/vuls/id/520827`
`url: https://bugs.php.net/bug.php?id=61910`
`url: https://www.php.net/manual/en/security.cgi-bin.php`
`url: https://web.archive.org/web/20210121223743/http://www.securityfocus.com/bid/53388`
`url: https://web.archive.org/web/20120709064615/http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-risks-Update-2-1567532.html`
`url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog`
`cisa: Known Exploited Vulnerability (KEV) catalog`
`dfn-cert: DFN-CERT-2013-1494`
`dfn-cert: DFN-CERT-2012-1316`
`dfn-cert: DFN-CERT-2012-1276`
`dfn-cert: DFN-CERT-2012-1268`
`dfn-cert: DFN-CERT-2012-1267`
`dfn-cert: DFN-CERT-2012-1266`
`dfn-cert: DFN-CERT-2012-1173`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-1101
dfn-cert: DFN-CERT-2012-0994
dfn-cert: DFN-CERT-2012-0993
dfn-cert: DFN-CERT-2012-0992
dfn-cert: DFN-CERT-2012-0920
dfn-cert: DFN-CERT-2012-0915
dfn-cert: DFN-CERT-2012-0914
dfn-cert: DFN-CERT-2012-0913
dfn-cert: DFN-CERT-2012-0907
dfn-cert: DFN-CERT-2012-0906
dfn-cert: DFN-CERT-2012-0900
dfn-cert: DFN-CERT-2012-0880
dfn-cert: DFN-CERT-2012-0878
```

[ return to 172.20.1.18 ]

### 2.5.2 Medium 5693/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

**Summary**
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**

```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
-------------------------------------------------------------------------------
↪-----------------------------------------------
TLSv1.2          | 10
```

**Impact**
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

**Solution:**
**Solution type:** VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

**Affected Software/OS**

... continues on next page ...

... continued from previous page ...

Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

**Vulnerability Insight**
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

**Vulnerability Detection Method**
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: `2024-09-27T05:05:23Z`

**References**
`cve: CVE-2011-1473`
`cve: CVE-2011-5094`
`url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego`
`↪tiation-dos/`
`url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/`
`url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation`
`url: https://www.openwall.com/lists/oss-security/2011/07/08/2`
`cert-bund: WID-SEC-2024-1591`
`cert-bund: WID-SEC-2024-0796`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K17/0980`
`cert-bund: CB-K17/0979`
`cert-bund: CB-K14/0772`
`cert-bund: CB-K13/0915`
`cert-bund: CB-K13/0462`
`dfn-cert: DFN-CERT-2017-1013`
`dfn-cert: DFN-CERT-2017-1012`
`dfn-cert: DFN-CERT-2014-0809`
`dfn-cert: DFN-CERT-2013-1928`
`dfn-cert: DFN-CERT-2012-1112`

[ return to 172.20.1.18 ]

### 2.5.3 Medium 80/tcp

Medium (CVSS: 5.3)
NVT: phpinfo() Output Reporting (HTTP)

**Summary**
Reporting of files containing the output of the phpinfo() PHP function previously detected via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information:
http://172.20.1.18/php/info.php
Concluded from:
  <title>PHP 7.4.33 - phpinfo()</title>
  <tr><td class="e">Configuration File (php.ini) Path </td>
  <h2>PHP Variables</h2>
http://172.20.1.18/php/info.php
Concluded from:
  <title>PHP 7.4.33 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFO
↪LLOW,NOARCHIVE" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↪p/7.4/apache2 </td></tr>
  <h2>PHP Variables</h2>
http://172.20.1.18/phpinfo.php
Concluded from:
  <title>PHP 7.4.33 - phpinfo()</title>
  <tr><td class="e">Configuration File (php.ini) Path </td>
  <h2>PHP Variables</h2>
http://172.20.1.18/phpinfo.php
Concluded from:
  <title>PHP 7.4.33 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFO
↪LLOW,NOARCHIVE" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↪p/7.4/apache2 </td></tr>
  <h2>PHP Variables</h2>
```

**Impact**
Some of the information that can be gathered from this file includes:
The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.

**Solution:**
**Solution type:** Workaround
Delete the listed files or restrict access to them.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
All systems exposing a file containing the output of the phpinfo() PHP function.
This VT is also reporting if an affected endpoint for the following products have been identified:
- CVE-2008-0149: TUTOS
- CVE-2023-49282, CVE-2023-49283: Microsoft Graph PHP SDK

**Vulnerability Insight**
Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory.

**Vulnerability Detection Method**
This script reports files identified by the following separate VT: 'phpinfo() Output Detection (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.108474).
Details: `phpinfo() Output Reporting (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: `2024-12-17T05:05:41Z`

**References**
`cve: CVE-2008-0149`
`cve: CVE-2023-49282`
`cve: CVE-2023-49283`
`url: https://www.php.net/manual/en/function.phpinfo.php`

Medium (CVSS: 5.0)
NVT: Sensitive File Disclosure (HTTP)

**Summary**
The script attempts to identify files containing sensitive data at the remote web server.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
```
The following files containing sensitive information were identified:
Description:   Microsoft IIS / ASP.NET Core Module web.config file accessible. T
↪his could contain sensitive information about the structure of the application
↪ / web server and shouldn't be accessible.
Match:         <configuration>
  <system.webServer>
Used regex:    ^\s*<(configuration|system\.web(Server)?)>
Extra match 1:   </system.webServer>
</configuration>
Used regex:    ^\s*</(configuration|system\.web(Server)?)>
URL:           http://172.20.1.18/cic/web.config
```

**Impact**

... continues on next page ...

... continued from previous page ...

Based on the information provided in these files an attacker might be able to gather additional info and/or sensitive data like usernames and passwords.

**Solution:**
**Solution type:** Mitigation
The sensitive files shouldn't be accessible via a web server. Restrict access to it or remove it completely.

**Vulnerability Insight**
Currently the script is checking for files like e.g.:
- Software (Blog, CMS) configuration or log files
- Web / application server configuration / password files (.htaccess, .htpasswd, web.config, web.xml, ...)
- Cloud (e.g. AWS) configuration files
- Files containing API keys for services / providers
- Database backup files
- Editor / history files
- SSH or SSL/TLS Private Keys

**Vulnerability Detection Method**
Enumerate the remote web server and check if sensitive files are accessible.
Details: `Sensitive File Disclosure (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.107305
Version used: `2024-06-12T05:05:44Z`

[ return to 172.20.1.18 ]

### 2.5.4 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↪)`

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The remote SSH server supports the following weak client-to-server MAC algorithm`

... continues on next page ...

... continued from previous page ...

```
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[ return to 172.20.1.18 ]

## 2.6 172.20.1.2

| | |
|---|---|
| Host scan start | Thu Feb 13 08:27:51 2025 UTC |
| Host scan end | Thu Feb 13 08:53:26 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 10000/tcp | High |
| 10000/tcp | Medium |
| 22/tcp | Medium |
| 22/tcp | Low |

### 2.6.1 High 10000/tcp

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2016-2183

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 172.20.1.2 ]

### 2.6.2 Medium 10000/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

**Solution:**
**Solution type:** Mitigation

... continues on next page ...

... continued from previous page ...

The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: `SSL/TLS: Report Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2013-2566`
`cve: CVE-2015-2808`
`cve: CVE-2015-4000`
`url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1`
`↪465_update_6.html`
`url: https://bettercrypto.org/`
`url: https://mozilla.github.io/server-side-tls/ssl-config-generator/`
`cert-bund: CB-K21/0067`
`cert-bund: CB-K19/0812`
`cert-bund: CB-K17/1750`
`cert-bund: CB-K16/1593`
`cert-bund: CB-K16/1552`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0617`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0168`
`cert-bund: CB-K16/0121`
`cert-bund: CB-K16/0090`
`cert-bund: CB-K16/0030`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1591`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

**Summary**

The remote server's SSL/TLS certificate has already expired.

... continues on next page ...

... continued from previous page ...

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
The certificate of the remote service expired on 2024-02-23 23:59:59.
Certificate details:
fingerprint (SHA-1)                | 025780AD3A22D0F12D4138F2522A8112E6B597BC
fingerprint (SHA-256)              | 309268CC450BDF9DCA94398785CBC36E80BAD68AEB085E
↪5A9CA23ECCB7E12E80
issued by                          | CN=Sectigo RSA Domain Validation Secure Server
↪ CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB
public key algorithm               | RSA
public key size (bits)             | 2048
serial                             | 00B44852541D5894C30F67A24DD2C9DE07
signature algorithm                | sha256WithRSAEncryption
subject                            | CN=*.univ-lome.tg
subject alternative names (SAN)    | *.univ-lome.tg, univ-lome.tg
valid from                         | 2023-01-23 00:00:00 UTC
valid until                        | 2024-02-23 23:59:59 UTC
```

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

[ return to 172.20.1.2 ]

### 2.6.3 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Product detection result**

... continues on next page ...

... continued from previous page ...

cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak KEX algorithm(s):

| KEX algorithm | Reason |
|---|---|
| diffie-hellman-group-exchange-sha1 | Using SHA-1 |
| diffie-hellman-group1-sha1 | Using Oakley Group 2 (a 1024-bit MODP group ↪) and SHA-1 |

**Impact**
An attacker can quickly break individual connections.

**Solution:**
**Solution type:** Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

**Vulnerability Insight**
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

**Vulnerability Detection Method**
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: 2024-06-14T05:05:48Z

... continues on next page ...

... continued from previous page ...

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak encryption algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc

**Solution:**
**Solution type:** Mitigation

... continues on next page ...

... continued from previous page ...

Disable the reported weak encryption algorithm(s).

**Vulnerability Insight**
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

**Vulnerability Detection Method**
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms
Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc8758`
`url: https://www.kb.cert.org/vuls/id/958563`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3`

[ return to 172.20.1.2 ]

### 2.6.4 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565`
`↪)`

... continues on next page ...

... continued from previous page ...

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[ return to 172.20.1.2 ]

## 2.7 172.20.1.201

| | |
|---|---|
| Host scan start | Thu Feb 13 15:31:26 2025 UTC |
| Host scan end | Thu Feb 13 16:33:24 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 21/tcp | Medium |
| 80/tcp | Medium |
| 22/tcp | Medium |
| general/tcp | Medium |
| 23/tcp | Medium |
| 22/tcp | Low |

### 2.7.1 Medium 21/tcp

Medium (CVSS: 6.4)
NVT: MikroTik RouterOS < 6.49.12, 7.x < 7.13.3 DoS Vulnerability (Loop DoS)

**Summary**
MikroTik RouterOS is prone to a denial of service (DoS) vulnerability dubbed 'Loop DoS'.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
Installed version: 7.8
Fixed version:     7.13.3
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 6.49.12, 7.13.3 or later.

**Affected Software/OS**
MikroTik RouterOS versions prior to 6.49.12 and 7.x through 7.13.2.

**Vulnerability Insight**
A vulnerability was found in the MikroTik RouterOS UPD protocol implementation. This issue may allow an unauthenticated attacker to send maliciously crafted packages leading to a denial of service on the targeted system.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `MikroTik RouterOS < 6.49.12, 7.x < 7.13.3 DoS Vulnerability (Loop DoS)`
OID:1.3.6.1.4.1.25623.1.0.103297
Version used: `2024-09-12T07:59:53Z`

... continues on next page ...

... continued from previous page ...

**References**
cve: CVE-2024-2169
url: https://mikrotik.com/download/changelogs
url: https://forum.mikrotik.com/viewtopic.php?t=206092
url: https://kb.cert.org/vuls/id/417980#MikroTik
url: https://cispa.de/en/loop-dos
url: https://cispa.saarland/group/rossow/Loop-DoS
url: https://github.com/cispa/loop-DoS
cert-bund: WID-SEC-2024-0672

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

**Summary**
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↪. Response(s):
Non-anonymous sessions: 331 Password required for gbvt
Anonymous sessions: 331 Password required for anonymous

**Impact**
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

**Solution:**
**Solution type:** Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

**Vulnerability Detection Method**
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: FTP Unencrypted Cleartext Login
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: 2023-12-20T05:05:58Z

[ return to 172.20.1.201 ]

### 2.7.2 Medium 80/tcp

Medium (CVSS: 6.4)
NVT: MikroTik RouterOS < 6.49.12, 7.x < 7.13.3 DoS Vulnerability (Loop DoS)

**Summary**
MikroTik RouterOS is prone to a denial of service (DoS) vulnerability dubbed 'Loop DoS'.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
Installed version: 7.8
Fixed version:     7.13.3
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 6.49.12, 7.13.3 or later.

**Affected Software/OS**
MikroTik RouterOS versions prior to 6.49.12 and 7.x through 7.13.2.

**Vulnerability Insight**
A vulnerability was found in the MikroTik RouterOS UPD protocol implementation. This issue may allow an unauthenticated attacker to send maliciously crafted packages leading to a denial of service on the targeted system.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `MikroTik RouterOS < 6.49.12, 7.x < 7.13.3 DoS Vulnerability (Loop DoS)`
OID:1.3.6.1.4.1.25623.1.0.103297
Version used: 2024-09-12T07:59:53Z

**References**
```
cve: CVE-2024-2169
url: https://mikrotik.com/download/changelogs
url: https://forum.mikrotik.com/viewtopic.php?t=206092
url: https://kb.cert.org/vuls/id/417980#MikroTik
url: https://cispa.de/en/loop-dos
url: https://cispa.saarland/group/rossow/Loop-DoS
url: https://github.com/cispa/loop-DoS
cert-bund: WID-SEC-2024-0672
```

[ return to 172.20.1.201 ]

### 2.7.3 Medium 22/tcp

Medium (CVSS: 6.4)
NVT: MikroTik RouterOS < 6.49.12, 7.x < 7.13.3 DoS Vulnerability (Loop DoS)

**Summary**
MikroTik RouterOS is prone to a denial of service (DoS) vulnerability dubbed 'Loop DoS'.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
Installed version: 7.8
Fixed version:     7.13.3
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 6.49.12, 7.13.3 or later.

**Affected Software/OS**
MikroTik RouterOS versions prior to 6.49.12 and 7.x through 7.13.2.

**Vulnerability Insight**
A vulnerability was found in the MikroTik RouterOS UPD protocol implementation. This issue may allow an unauthenticated attacker to send maliciously crafted packages leading to a denial of service on the targeted system.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `MikroTik RouterOS < 6.49.12, 7.x < 7.13.3 DoS Vulnerability (Loop DoS)`
OID:1.3.6.1.4.1.25623.1.0.103297
Version used: `2024-09-12T07:59:53Z`

**References**
```
cve: CVE-2024-2169
url: https://mikrotik.com/download/changelogs
url: https://forum.mikrotik.com/viewtopic.php?t=206092
url: https://kb.cert.org/vuls/id/417980#MikroTik
url: https://cispa.de/en/loop-dos
url: https://cispa.saarland/group/rossow/Loop-DoS
url: https://github.com/cispa/loop-DoS
cert-bund: WID-SEC-2024-0672
```

Medium (CVSS: 5.3)
NVT: Weak Host Key Algorithm(s) (SSH)

**Product detection result**
... continues on next page ...

... continued from previous page ...

cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak host key algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
---
↪---
ssh-dss | Digital Signature Algorithm (DSA) / Digital Signature Stand
↪ard (DSS)

**Solution:**
**Solution type:** Mitigation
Disable the reported weak host key algorithm(s).

**Vulnerability Detection Method**
Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: Weak Host Key Algorithm(s) (SSH)
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc8332
url: https://www.rfc-editor.org/rfc/rfc8709
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol

... continues on next page ...

... continued from previous page ...

Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                     | Reason
----------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

**Impact**
An attacker can quickly break individual connections.

**Solution:**
**Solution type:** Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

**Vulnerability Insight**
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

**Vulnerability Detection Method**
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak encryption algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc

**Solution:**
**Solution type:** Mitigation
Disable the reported weak encryption algorithm(s).

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

**Vulnerability Detection Method**
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms
Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc8758`
`url: https://www.kb.cert.org/vuls/id/958563`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3`

[ return to 172.20.1.201 ]

### 2.7.4 Medium general/tcp

Medium (CVSS: 5.3)
NVT: MikroTik RouterOS 7.1 < 7.12 Access Control Vulnerability

**Product detection result**
`cpe:/o:mikrotik:routeros:7.8`
`Detected by MikroTik RouterOS Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.`
`↪0.810608)`

**Summary**
MikroTik RouterOS is prone to an access control vulnerability in the REST API.

... continues on next page ...

... continued from previous page ...

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`Installed version: 7.8`
`Fixed version: 7.12`

**Solution:**
**Solution type:** VendorFix
Update to version 7.12 or later.

**Affected Software/OS**
MikroTik RouterOS version 7.1 through 7.11.

**Vulnerability Insight**
The vulnerability lies in the fact that, while other interfaces (SSH, Webfig, etc.) check whether the user is authorized to log in from that specific IP address, this is not the case for the REST server. Users can access the REST server from any IP address, even if they are not authorized in the users database.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `MikroTik RouterOS 7.1 < 7.12 Access Control Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.151303
Version used: `2023-11-24T16:09:32Z`

**Product Detection Result**
Product: `cpe:/o:mikrotik:routeros:7.8`
Method: `MikroTik RouterOS Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.810608)

**References**
`cve: CVE-2023-41570`
`url: https://www.enricobassetti.it/2023/11/cve-2023-41570-access-control-vulnera`
`↪bility-in-mikrotik-rest-api/`

[ return to 172.20.1.201 ]

### 2.7.5 Medium 23/tcp

Medium (CVSS: 4.8)
NVT: Telnet Unencrypted Cleartext Login

**Summary**

... continues on next page ...

... continued from previous page ...

The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.

**Solution:**
**Solution type:** Mitigation
Replace Telnet with a protocol like SSH which supports encrypted connections.

**Vulnerability Detection Method**
Details: `Telnet Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108522
Version used: `2023-10-13T05:06:09Z`

[ return to 172.20.1.201 ]

### 2.7.6 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↪)`

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
hmac-md5
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
hmac-md5
```

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[ return to 172.20.1.201 ]

## 2.8 172.20.1.250

Host scan start Thu Feb 13 08:33:12 2025 UTC
Host scan end Thu Feb 13 09:45:09 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 1883/tcp | Medium |
| 8883/tcp | Medium |
| 22/tcp | Low |

### 2.8.1 Medium 1883/tcp

Medium (CVSS: 6.4)
NVT: MQTT Broker Does Not Require Authentication

**Summary**
The remote MQTT broker does not require authentication.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Solution:**
**Solution type:** Mitigation
Enable authentication.

**Vulnerability Detection Method**
Checks if authentication is required for the remote MQTT broker.
Details: `MQTT Broker Does Not Require Authentication`
OID:1.3.6.1.4.1.25623.1.0.140167
Version used: `2022-07-11T10:16:03Z`

**References**
`url: https://www.heise.de/newsticker/meldung/MQTT-Protokoll-IoT-Kommunikation-vo`
`↪n-Reaktoren-und-Gefaengnissen-oeffentlich-einsehbar-3629650.html`

[ return to 172.20.1.250 ]

### 2.8.2 Medium 8883/tcp

Medium (CVSS: 6.4)
NVT: MQTT Broker Does Not Require Authentication

**Summary**
The remote MQTT broker does not require authentication.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Solution:**
**Solution type:** Mitigation
Enable authentication.

**Vulnerability Detection Method**
. . . continues on next page . . .

... continued from previous page ...

Checks if authentication is required for the remote MQTT broker.
Details: MQTT Broker Does Not Require Authentication
OID:1.3.6.1.4.1.25623.1.0.140167
Version used: 2022-07-11T10:16:03Z

**References**
url: https://www.heise.de/newsticker/meldung/MQTT-Protokoll-IoT-Kommunikation-vo
↪n-Reaktoren-und-Gefaengnissen-oeffentlich-einsehbar-3629650.html

[ return to 172.20.1.250 ]

### 2.8.3 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:

... continues on next page ...

... continued from previous page ...

- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm

Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[ return to 172.20.1.250 ]

## 2.9 172.20.1.71

Host scan start Thu Feb 13 07:22:48 2025 UTC
Host scan end Thu Feb 13 08:27:45 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | Medium |
| 5432/tcp | Medium |
| 22/tcp | Low |

### 2.9.1 Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Unprotected Web App / Device Installers (HTTP)

**Summary**
The script attempts to identify installation/setup pages of various web apps/devices that are publicly accessible and not protected by e.g. account restrictions or having their setup finished.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The following web app/device installers are unprotected/have not finished their ↪setup and are publicly accessible (URL:Description):`
`http://172.20.1.71/phpmyadmin/setup/index.php - CubeCart / phpMyAdmin installer`

... continues on next page ...

... continued from previous page ...

http://172.20.1.71/phpMyAdmin/setup/index.php - CubeCart / phpMyAdmin installer

**Impact**
It is possible to install or reconfigure the software. In doing so, the attacker could overwrite existing configurations. It could be possible for the attacker to gain access to the base system

**Solution:**
**Solution type:** Mitigation
Setup and/or installation pages for Web Apps should not be publicly accessible via a web server. Restrict access to it, remove it completely or finish the setup of the application / device.

**Vulnerability Detection Method**
Enumerate the remote web server and check if unprotected web apps/devices are accessible for installation.
Details: Unprotected Web App / Device Installers (HTTP)
OID:1.3.6.1.4.1.25623.1.0.107307
Version used: 2024-11-29T05:05:36Z

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The following input fields were identified (URL:input name):
http://172.20.1.71/phpMyAdmin/:pma_password
http://172.20.1.71/phpMyAdmin/?D=A:pma_password
http://172.20.1.71/phpmyadmin/:pma_password
http://172.20.1.71/phpmyadmin/?D=A:pma_password

**Impact**
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

**References**
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[ return to 172.20.1.71 ]

### 2.9.2 Medium 5432/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.`
`↪802067)`

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
`'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:`
`TLS_RSA_WITH_SEED_CBC_SHA`

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: `SSL/TLS: Report Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2013-2566`
`cve: CVE-2015-2808`
`cve: CVE-2015-4000`
`url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1`
`↪465_update_6.html`
`url: https://bettercrypto.org/`
`url: https://mozilla.github.io/server-side-tls/ssl-config-generator/`
`cert-bund: CB-K21/0067`
`cert-bund: CB-K19/0812`
`cert-bund: CB-K17/1750`
`cert-bund: CB-K16/1593`
`cert-bund: CB-K16/1552`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0617`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0168`
`cert-bund: CB-K16/0121`
`cert-bund: CB-K16/0090`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

[ return to 172.20.1.71 ]

### 2.9.3 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol

... continues on next page ...

... continued from previous page ...

Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[ return to 172.20.1.71 ]

## 2.10 172.20.1.252

| | |
|---|---|
| Host scan start | Thu Feb 13 08:53:31 2025 UTC |
| Host scan end | Thu Feb 13 12:17:58 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 465/tcp | Medium |
| 110/tcp | Medium |
| 587/tcp | Medium |
| 25/tcp | Medium |
| 143/tcp | Medium |
| 8443/tcp | Medium |
| 22/tcp | Low |

### 2.10.1 Medium 465/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.`
`↪802067)`

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
`'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:`
`TLS_RSA_WITH_SEED_CBC_SHA`

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)

. . . continues on next page . . .

... continued from previous page ...

- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977

Medium (CVSS: 5.4)
NVT: SSL/TLS: Report 'Anonymous' Cipher Suites

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all 'Anonymous' SSL/TLS cipher suites accepted by a service.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA256
TLS_DH_anon_WITH_AES_128_GCM_SHA256
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA256

... continues on next page ...

... continued from previous page ...

TLS_DH_anon_WITH_AES_256_GCM_SHA384
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
TLS_DH_anon_WITH_SEED_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA

**Impact**
This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed 'Anonymous' cipher suites anymore.
Please see the references for more resources supporting you in this task.

**Vulnerability Insight**
Services supporting 'Anonymous' cipher suites could allow a client to negotiate an SSL/TLS connection to the host without any authentication of the remote endpoint.

**Vulnerability Detection Method**
Details: SSL/TLS: Report 'Anonymous' Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.108147
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2007-1858
cve: CVE-2014-0351
url: https://bettercrypto.org/
url: http://www.securityfocus.com/bid/28482
url: http://www.securityfocus.com/bid/69754
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K14/0058
dfn-cert: DFN-CERT-2014-0049
dfn-cert: DFN-CERT-2012-0442

[ return to 172.20.1.252 ]

### 2.10.2 Medium 110/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

**Summary**
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**

```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪----------------------------------------------
TLSv1.2          | 10
```

**Impact**
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

**Solution:**
**Solution type:** VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

**Affected Software/OS**
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

**Vulnerability Insight**
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

**Vulnerability Detection Method**
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: `2024-09-27T05:05:23Z`

. . . continues on next page . . .

... continued from previous page ...

**References**

cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego
↪tiation-dos/
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
url: https://www.openwall.com/lists/oss-security/2011/07/08/2
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-0796
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K17/0980
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112

[ return to 172.20.1.252 ]

### 2.10.3 Medium 587/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**

cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**

This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_SEED_CBC_SHA

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: `SSL/TLS: Report Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2013-2566`
`cve: CVE-2015-2808`
`cve: CVE-2015-4000`
`url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1`
`↪465_update_6.html`
`url: https://bettercrypto.org/`
`url: https://mozilla.github.io/server-side-tls/ssl-config-generator/`
`cert-bund: CB-K21/0067`
`cert-bund: CB-K19/0812`
`cert-bund: CB-K17/1750`
`cert-bund: CB-K16/1593`
`cert-bund: CB-K16/1552`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0617`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0168`
`cert-bund: CB-K16/0121`
`cert-bund: CB-K16/0090`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

**Summary**
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
`The following indicates that the remote SSL/TLS service is affected:`

... continues on next page ...

... continued from previous page ...

```
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪-------------------------------------------------
TLSv1.2          | 10
```

**Impact**
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

**Solution:**
**Solution type:** VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

**Affected Software/OS**
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

**Vulnerability Insight**
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

**Vulnerability Detection Method**
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: `2024-09-27T05:05:23Z`

**References**
```
cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego
↪tiation-dos/
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
url: https://www.openwall.com/lists/oss-security/2011/07/08/2
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-0796
cert-bund: WID-SEC-2023-1435
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K17/0980
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112
```

[ return to 172.20.1.252 ]

### 2.10.4 Medium 25/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

**Summary**
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**

```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪----------------------------------------------
TLSv1.2          | 10
```

**Impact**
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

**Solution:**
**Solution type:** VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

**Affected Software/OS**
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

**Vulnerability Detection Method**
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: `2024-09-27T05:05:23Z`

**References**
`cve: CVE-2011-1473`
`cve: CVE-2011-5094`
`url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego`
`↪tiation-dos/`
`url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/`
`url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation`
`url: https://www.openwall.com/lists/oss-security/2011/07/08/2`
`cert-bund: WID-SEC-2024-1591`
`cert-bund: WID-SEC-2024-0796`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K17/0980`
`cert-bund: CB-K17/0979`
`cert-bund: CB-K14/0772`
`cert-bund: CB-K13/0915`
`cert-bund: CB-K13/0462`
`dfn-cert: DFN-CERT-2017-1013`
`dfn-cert: DFN-CERT-2017-1012`
`dfn-cert: DFN-CERT-2014-0809`
`dfn-cert: DFN-CERT-2013-1928`
`dfn-cert: DFN-CERT-2012-1112`

[ return to 172.20.1.252 ]

### 2.10.5 Medium 143/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

**Summary**
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

... continues on next page ...

... continued from previous page ...

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**

```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
-------------------------------------------------------------------------------
↪-----------------------------------------------
TLSv1.2          | 10
```

**Impact**

The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

**Solution:**

**Solution type:** VendorFix

Users should contact their vendors for specific patch information.

A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

**Affected Software/OS**

Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

**Vulnerability Insight**

The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.

Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:

> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.

Both CVEs are still kept in this VT as a reference to the origin of this flaw.

**Vulnerability Detection Method**

Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.

Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`

OID:1.3.6.1.4.1.25623.1.0.117761

Version used: `2024-09-27T05:05:23Z`

**References**

```
cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego
↪tiation-dos/
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
```

... continues on next page ...

... continued from previous page ...

```
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
url: https://www.openwall.com/lists/oss-security/2011/07/08/2
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-0796
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K17/0980
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112
```

[ return to 172.20.1.252 ]

### 2.10.6 Medium 8443/tcp

Medium (CVSS: 5.0)
NVT: Backup File Scanner (HTTP) - Reliable Detection Reporting

**Summary**
The script reports backup files left on the web server.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The following backup files were identified (<URL>:<Matching pattern>):`
`https://172.20.1.252:8443/config/config.inc.php.orig:^<\?(php|=)`

**Impact**
Based on the information provided in these files an attacker might be able to gather sensitive information stored in these files.

**Solution:**
**Solution type:** Mitigation
Delete the backup files.

**Vulnerability Insight**
Notes:
- 'Reliable Detection' means that a file was detected based on a strict (regex) and reliable pattern matching the response of the remote web server when a file was requested.

... continues on next page ...

... continued from previous page ...

- As the VT 'Backup File Scanner (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.140853) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

**Vulnerability Detection Method**
Reports previous enumerated backup files accessible on the remote web server.
Details: `Backup File Scanner (HTTP) - Reliable Detection Reporting`
OID:1.3.6.1.4.1.25623.1.0.108976
Version used: `2022-09-13T10:15:09Z`

**References**
`url: http://www.openwall.com/lists/oss-security/2017/10/31/1`

[ return to 172.20.1.252 ]

### 2.10.7 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↪)`

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s):`
`umac-64-etm@openssh.com`
`umac-64@openssh.com`
`The remote SSH server supports the following weak server-to-client MAC algorithm ↪(s):`
`umac-64-etm@openssh.com`
`umac-64@openssh.com`

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**

... continues on next page ...

... continued from previous page ...

Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[ return to 172.20.1.252 ]

## 2.11 172.20.1.3

| | |
|---|---|
| Host scan start | Thu Feb 13 08:33:57 2025 UTC |
| Host scan end | Thu Feb 13 09:49:02 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 22/tcp | Medium |

### 2.11.1 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565`
`↪)`

**Summary**
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

... continues on next page ...

... continued from previous page ...

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                     | Reason
-------------------------------------------------
diffie-hellman-group-exchange-sha1 | Using SHA-1
```

**Impact**

An attacker can quickly break individual connections.

**Solution:**

**Solution type:** Mitigation

Disable the reported weak KEX algorithm(s)

- 1024-bit MODP group / prime KEX algorithms:

Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

**Vulnerability Insight**

- 1024-bit MODP group / prime KEX algorithms:

Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.

A nation-state can break a 1024-bit prime.

**Vulnerability Detection Method**

Checks the supported KEX algorithms of the remote SSH server.

Currently weak KEX algorithms are defined as the following:

- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key

Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`

OID:1.3.6.1.4.1.25623.1.0.150713

Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**

Product: `cpe:/a:ietf:secure_shell_protocol`

Method: `SSH Protocol Algorithms Supported`

OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**

```
url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
```

... continues on next page ...

... continued from previous page ...

url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak encryption algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
aes128-cbc
aes256-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
aes128-cbc
aes256-cbc

**Solution:**
**Solution type:** Mitigation
Disable the reported weak encryption algorithm(s).

**Vulnerability Insight**
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

**Vulnerability Detection Method**
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms

... continues on next page ...

... continued from previous page ...

Details: Weak Encryption Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc8758
url: https://www.kb.cert.org/vuls/id/958563
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3

[ return to 172.20.1.3 ]

## 2.12 172.20.1.60

Host scan start Thu Feb 13 07:22:48 2025 UTC
Host scan end Thu Feb 13 08:37:33 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | Medium |
| 443/tcp | Medium |
| 22/tcp | Low |

### 2.12.1 Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Nagios XI < 2011R1.9 Multiple XSS Vulnerabilities - Active Check

**Summary**
Nagios XI is prone to multiple cross-site scripting (XSS) vulnerabilities.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
Vulnerable URL: http://172.20.1.60/nagiosxi/login.php/";alert(document.cookie);"

**Impact**
Successful exploitation will allow remote attackers to insert arbitrary HTML and script code, which will be executed in a user's browser session in the context of an affected site.

**Solution:**

... continues on next page ...

... continued from previous page ...

**Solution type:** VendorFix
Update to version 2011R1.9 or later.

**Affected Software/OS**
Nagios XI prior to version 2011R1.9.

**Vulnerability Insight**
Multiple flaws are due to improper validation of user-supplied input appended to the URL in multiple scripts, which allows attackers to execute arbitrary HTML and script code in a user's browser session in the context of an affected site.

**Vulnerability Detection Method**
Sends a crafted HTTP GET request and checks the response.
Details: `Nagios XI < 2011R1.9 Multiple XSS Vulnerabilities - Active Check`
OID:1.3.6.1.4.1.25623.1.0.902599
Version used: `2023-12-01T05:05:39Z`

**References**
`url: http://www.nagios.com/products/nagiosxi`
`url: http://www.securityfocus.com/bid/51069`
`url: http://xforce.iss.net/xforce/xfdb/71825`
`url: http://xforce.iss.net/xforce/xfdb/71826`
`url: http://seclists.org/fulldisclosure/2011/Dec/354`
`url: http://packetstormsecurity.org/files/107872/0A29-11-3.txt`

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The following URLs requires Basic Authentication (URL:realm name):`
`http://172.20.1.60/nagios:"Nagios Core"`

**Impact**
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround

... continues on next page ...

... continued from previous page ...

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

**References**
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[ return to 172.20.1.60 ]

### 2.12.2 Medium 443/tcp

Medium (CVSS: 5.0)
NVT: Nagios XI < 2011R1.9 Multiple XSS Vulnerabilities - Active Check

**Summary**
Nagios XI is prone to multiple cross-site scripting (XSS) vulnerabilities.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
`Vulnerable URL: https://172.20.1.60/nagiosxi/login.php/";alert(document.cookie);`
`↪"`

**Impact**
Successful exploitation will allow remote attackers to insert arbitrary HTML and script code, which will be executed in a user's browser session in the context of an affected site.

**Solution:**

... continues on next page ...

... continued from previous page ...

**Solution type:** VendorFix
Update to version 2011R1.9 or later.

**Affected Software/OS**
Nagios XI prior to version 2011R1.9.

**Vulnerability Insight**
Multiple flaws are due to improper validation of user-supplied input appended to the URL in multiple scripts, which allows attackers to execute arbitrary HTML and script code in a user's browser session in the context of an affected site.

**Vulnerability Detection Method**
Sends a crafted HTTP GET request and checks the response.
Details: `Nagios XI < 2011R1.9 Multiple XSS Vulnerabilities - Active Check`
OID:1.3.6.1.4.1.25623.1.0.902599
Version used: `2023-12-01T05:05:39Z`

**References**
`url: http://www.nagios.com/products/nagiosxi`
`url: http://www.securityfocus.com/bid/51069`
`url: http://xforce.iss.net/xforce/xfdb/71825`
`url: http://xforce.iss.net/xforce/xfdb/71826`
`url: http://seclists.org/fulldisclosure/2011/Dec/354`
`url: http://packetstormsecurity.org/files/107872/0A29-11-3.txt`

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              CN=192.168.210.71,OU=Development,O=Nagios Enterprises,L=St
↪. Paul,ST=Minnesota,C=US
Signature Algorithm:  sha1WithRSAEncryption
```

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

**References**
`url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/`

[ return to 172.20.1.60 ]

### 2.12.3 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)`

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[ return to 172.20.1.60 ]

## 2.13 172.20.1.6

| | |
|---|---|
| Host scan start | Thu Feb 13 09:26:50 2025 UTC |
| Host scan end | Thu Feb 13 10:48:16 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 8181/tcp | Medium |
| 22/tcp | Low |

### 2.13.1 Medium 8181/tcp

Medium (CVSS: 5.0)
NVT: Source Control Management (SCM) Files/Folders Accessible (HTTP)

**Summary**
The script attempts to identify files/folders of a SCM accessible at the webserver.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**

```
The following SCM files/folders were identified:
Match:      0000000000000000000000000000000000000000 c6e727732a7f3f1060b1c1fbd78
↪75746db5f1000 root <root@moniteur.univ-lome.tg> 1695925148 +0000
clone: from g
↪it://git.moodle.org/moodle.git
c6e727732a7f3f1060b1c1fbd7875746db5f1000 da9ebc40f66f3a4a44c3f888a0d8318ee86e172
↪a root <root@moniteur.univ-lome.tg> 1695925233 +0000 checkout: moving from mas
↪ter to MOODLE_402_STABLE
Used regex: ^[a-f0-9]{40} [a-f0-9]{40}
URL:        https://172.20.1.6:8181/.git/logs/HEAD
Match:      [core]
[remote "origin"]
[branch "master"]
[branch "MOODLE_402_STABLE"]
Used regex: ^\[(core|receive|(remote|branch) .+)\]$
URL:        https://172.20.1.6:8181/.git/config
Match:      # git ls-files --others --exclude-from=.git/info/exclude
Used regex: ^# git ls-files
URL:        https://172.20.1.6:8181/.git/info/exclude
Match:      DIRC
Used regex: ^DIRC
URL:        https://172.20.1.6:8181/.git/index
Match:      Unnamed repository; edit this file 'description' to name the reposit
↪ory.
Used regex: ^Unnamed repository
URL:        https://172.20.1.6:8181/.git/description
Match:      ref: refs/heads/MOODLE_402_STABLE
Used regex: ^ref: refs/
URL:        https://172.20.1.6:8181/.git/HEAD
```

**Impact**

. . . continues on next page . . .

... continued from previous page ...

Based on the information provided in these files/folders an attacker might be able to gather additional info about the structure of the system and its applications.

**Solution:**
**Solution type:** Mitigation
Restrict access to the SCM files/folders for authorized systems only.

**Vulnerability Insight**
Currently the script is checking for files/folders of the following SCM software:
- Git (.git)
- Mercurial (.hg)
- Bazaar (.bzr)
- CVS (CVS/Root, CVS/Entries)
- Subversion (.svn)

**Vulnerability Detection Method**
Check the response if SCM files/folders are accessible.
Details: `Source Control Management (SCM) Files/Folders Accessible (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.111084
Version used: `2023-08-01T13:29:10Z`

**References**
`url: http://pen-testing.sans.org/blog/pen-testing/2012/12/06/all-your-svn-are-be`
`↪long-to-us`
`url: https://github.com/anantshri/svn-extractor`
`url: https://blog.skullsecurity.org/2012/using-git-clone-to-get-pwn3d`
`url: https://blog.netspi.com/dumping-git-data-from-misconfigured-web-servers/`
`url: http://resources.infosecinstitute.com/hacking-svn-git-and-mercurial/`

[ return to 172.20.1.6 ]

### 2.13.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565`
`↪)`

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

... continues on next page ...

... continued from previous page ...

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[ return to 172.20.1.6 ]

## 2.14 172.20.1.21

| | |
|---|---|
| Host scan start | Thu Feb 13 09:49:02 2025 UTC |
| Host scan end | Thu Feb 13 12:00:12 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 3000/tcp | Medium |
| 22/tcp | Low |

### 2.14.1 Medium 3000/tcp

Medium (CVSS: 5.0)
NVT: Express NODE_ENV 'development' Information Disclosure Vulnerability (HTTP) - Active Check

**Summary**
Express is prone to an information disclosure vulnerability if the NODE_ENV environment variable is set to 'development'.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**

```
By doing the following HTTP request:
GET / HTTP/1.1
Host: 172.20.1.21:3000
Content-Type: application/json
Connection: close
Content-Length: 14
gbvt1337794958
it was possible to trigger the following stacktrace / response including sensiti
↪ve application information:
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Error</title>
</head>
<body>
<pre>SyntaxError: Unexpected token g in JSON at position 0<br>    at J
↪SON.parse (&lt;anonymous&gt;)<br>    at createStrictSyntaxError (/ho
↪me/epl/workspace/site-collecte-docker/containers/nodejs/app/node_modules/body-
↪parser/lib/types/json.js:169:10)<br>    at parse (/home/epl/workspac
↪e/site-collecte-docker/containers/nodejs/app/node_modules/body-parser/lib/type
↪s/json.js:86:15)<br>    at /home/epl/workspace/site-collecte-docker/
↪containers/nodejs/app/node_modules/body-parser/lib/read.js:128:18<br>   &
↪nbsp;at AsyncResource.runInAsyncScope (node:async_hooks:203:9)<br>   &nbs
↪p;at invokeCallback (/home/epl/workspace/site-collecte-docker/containers/nodej
↪s/app/node_modules/raw-body/index.js:238:16)<br>    at done (/home/e
↪pl/workspace/site-collecte-docker/containers/nodejs/app/node_modules/raw-body/
↪index.js:227:7)<br>    at IncomingMessage.onEnd (/home/epl/workspace
↪/site-collecte-docker/containers/nodejs/app/node_modules/raw-body/index.js:287
↪:7)<br>    at IncomingMessage.emit (node:events:514:28)<br>   &
```

... continues on next page ...

... continued from previous page ...

```
↪nbsp;at endReadableNT (node:internal/streams/readable:1359:12)</pre>
</body>
</html>
```

**Impact**
In development mode, Express returns more verbose errors which can result in information leakage.

**Solution:**
**Solution type:** Mitigation
Set the NODE_ENV environment variable to 'production'. Please see the references for more information.

**Affected Software/OS**
Express applications having the NODE_ENV environment variable set to the 'development' default.

**Vulnerability Insight**
By default, Express applications run in development mode unless the NODE_ENV environmental variable is set to another value.

**Vulnerability Detection Method**
Sends a crafted HTTP GET request and checks the response.
Details: `Express NODE_ENV 'development' Information Disclosure Vulnerability (HTTP) - Ac.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.114542
Version used: 2024-06-10T05:05:40Z

**References**
`url: https://expressjs.com/en/advanced/best-practice-performance.html#set-node_e`
`↪nv-to-production`
`url: https://www.synopsys.com/blogs/software-security/nodejs-mean-stack-vulnerab`
`↪ilities.html`

[ return to 172.20.1.21 ]

### 2.14.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565`
`↪)`

... continues on next page ...

... continued from previous page ...

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
```
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4
```

[ return to 172.20.1.21 ]

## 2.15 172.20.1.24

| | |
|---|---|
| Host scan start | Thu Feb 13 10:37:50 2025 UTC |
| Host scan end | Thu Feb 13 15:34:25 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 5693/tcp | Medium |
| 443/tcp | Medium |
| 22/tcp | Low |

### 2.15.1 Medium 5693/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

**Summary**
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**

```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪----------------------------------------------
TLSv1.2          | 10
```

**Impact**
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

**Solution:**
**Solution type:** VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

**Affected Software/OS**
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

**Vulnerability Insight**
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:

. . . continues on next page . . .

... continued from previous page ...

> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

**Vulnerability Detection Method**
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: `2024-09-27T05:05:23Z`

**References**
`cve: CVE-2011-1473`
`cve: CVE-2011-5094`
`url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego`
`↪tiation-dos/`
`url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/`
`url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation`
`url: https://www.openwall.com/lists/oss-security/2011/07/08/2`
`cert-bund: WID-SEC-2024-1591`
`cert-bund: WID-SEC-2024-0796`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K17/0980`
`cert-bund: CB-K17/0979`
`cert-bund: CB-K14/0772`
`cert-bund: CB-K13/0915`
`cert-bund: CB-K13/0462`
`dfn-cert: DFN-CERT-2017-1013`
`dfn-cert: DFN-CERT-2017-1012`
`dfn-cert: DFN-CERT-2014-0809`
`dfn-cert: DFN-CERT-2013-1928`
`dfn-cert: DFN-CERT-2012-1112`

[ return to 172.20.1.24 ]

### 2.15.2 Medium 443/tcp

Medium (CVSS: 5.0)
NVT: Missing 'HttpOnly' Cookie Attribute (HTTP)

**Summary**
The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP cookie.

**Quality of Detection (QoD):** 70%

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**
The cookie(s):
Set-Cookie: pll_language=fr; expires=Fri, 13-Feb-2026 10:39:33 GMT; Max-Age=***r
↪eplaced***; path=/; secure; SameSite=Lax
is/are missing the "HttpOnly" cookie attribute.

**Solution:**
**Solution type:** Mitigation
- Set the 'HttpOnly' cookie attribute for any session cookie
- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

**Affected Software/OS**
Any web application with session handling in cookies.

**Vulnerability Insight**
The flaw exists if a session cookie is not using the 'HttpOnly' cookie attribute.
This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

**Vulnerability Detection Method**
Checks all cookies sent by the remote HTTP web server / application for a missing 'HttpOnly' cookie attribute.
Details: Missing 'HttpOnly' Cookie Attribute (HTTP)
OID:1.3.6.1.4.1.25623.1.0.105925
Version used: 2024-01-12T16:12:12Z

**References**
url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6
url: https://owasp.org/www-community/HttpOnly
url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0
↪02)

[ return to 172.20.1.24 ]

### 2.15.3 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

... continues on next page ...

... continued from previous page ...

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
```
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4
```

[ return to 172.20.1.24 ]

## 2.16 172.20.1.9

| | |
|---|---|
| Host scan start | Thu Feb 13 12:00:12 2025 UTC |
| Host scan end | Thu Feb 13 14:24:19 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | Medium |
| 22/tcp | Low |

### 2.16.1 Medium 443/tcp

Medium (CVSS: 5.0)
NVT: Missing 'HttpOnly' Cookie Attribute (HTTP)

**Summary**
The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP cookie.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
`The cookie(s):`
`Set-Cookie: PHPSESSID=***replaced***; path=/`
`is/are missing the "HttpOnly" cookie attribute.`

**Solution:**
**Solution type:** Mitigation
- Set the 'HttpOnly' cookie attribute for any session cookie
- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

**Affected Software/OS**
Any web application with session handling in cookies.

**Vulnerability Insight**
The flaw exists if a session cookie is not using the 'HttpOnly' cookie attribute.
This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

**Vulnerability Detection Method**
Checks all cookies sent by the remote HTTP web server / application for a missing 'HttpOnly' cookie attribute.
Details: `Missing 'HttpOnly' Cookie Attribute (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.105925
Version used: `2024-01-12T16:12:12Z`

**References**

. . . continues on next page . . .

... continued from previous page ...

url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6
url: https://owasp.org/www-community/HttpOnly
url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0
↪02)

Medium (CVSS: 5.0)
NVT: Missing 'Secure' Cookie Attribute (HTTP)

**Summary**
The remote HTTP web server / application is missing to set the 'Secure' cookie attribute for one or more sent HTTP cookie.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
The cookie(s):
Set-Cookie: PHPSESSID=***replaced***; path=/
is/are missing the "Secure" cookie attribute.

**Solution:**
**Solution type:** Mitigation
- Set the 'Secure' cookie attribute for any cookies that are sent over a SSL/TLS connection
- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

**Affected Software/OS**
Any web application accessible via a SSL/TLS connection (HTTPS) and at the same time also accessible over a cleartext connection (HTTP).

**Vulnerability Insight**
The flaw exists if a cookie is not using the 'Secure' cookie attribute and is sent over a SSL/TLS connection.
This allows a cookie to be passed to the server by the client over non-secure channels (HTTP) and subsequently allows an attacker to e.g. conduct session hijacking attacks.

**Vulnerability Detection Method**
Checks all cookies sent by the remote HTTP web server / application over a SSL/TLS connection for a missing 'Secure' cookie attribute.
Details: Missing 'Secure' Cookie Attribute (HTTP)
OID:1.3.6.1.4.1.25623.1.0.902661
Version used: 2024-09-27T05:05:23Z

**References**
url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.5
url: https://owasp.org/www-community/controls/SecureCookieAttribute

... continues on next page ...

... continued from previous page ...

url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0
↪02)

[ return to 172.20.1.9 ]

### 2.16.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610

... continues on next page ...

... continued from previous page ...

Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[ return to 172.20.1.9 ]

## 2.17 172.20.1.55

Host scan start Thu Feb 13 13:53:59 2025 UTC
Host scan end Thu Feb 13 15:31:26 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | Medium |
| 22/tcp | Low |

### 2.17.1 Medium 443/tcp

Medium (CVSS: 5.0)
NVT: Missing 'HttpOnly' Cookie Attribute (HTTP)

**Summary**
The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP cookie.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
The cookie(s):
Set-Cookie: XSRF-TOKEN=eyJpdiI6InM0ei81UFBCOENNNWJocHgrcUdHOUE9PSIsInZhbHVlIjoid
↪FI2MFRPQmYzY3l6Y3BSQ0p2ZVUyY0U0WW01cUpERVJ4MVhNekZFZkdYbHF4bU1RbW5URjg2bUd6R3F
↪0WUZqRnVuaGJhNUF2UElrM2kxRjU5eC9zVkVmeVd6TU4yWEc3RE9qS0hETWFBMHBzWEx1aWluVVphM
↪XdRb1FDRW9xa2EiLCJtYWMiOiIzZjMxNTI1ZGQwNWU0MmJkZGU2OGI2YzM3MDg3OTRkNzBlYjg3NDE
↪zODJjYmVmMTIyMjkxMzk2ZjQ0MGJhM2FjIiwidGFnIjoiIn0%3D; expires=Thu, 13 Feb 2025
↪15:54:44 GMT; Max-Age=***replaced***; path=/; samesite=lax
is/are missing the "HttpOnly" cookie attribute.

**Solution:**

... continues on next page ...

... continued from previous page ...

**Solution type:** Mitigation
- Set the 'HttpOnly' cookie attribute for any session cookie
- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

**Affected Software/OS**
Any web application with session handling in cookies.

**Vulnerability Insight**
The flaw exists if a session cookie is not using the 'HttpOnly' cookie attribute.
This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

**Vulnerability Detection Method**
Checks all cookies sent by the remote HTTP web server / application for a missing 'HttpOnly' cookie attribute.
Details: `Missing 'HttpOnly' Cookie Attribute (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.105925
Version used: `2024-01-12T16:12:12Z`

**References**
`url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6`
`url: https://owasp.org/www-community/HttpOnly`
`url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0`
`↪02)`

Medium (CVSS: 5.0)
NVT: Missing 'Secure' Cookie Attribute (HTTP)

**Summary**
The remote HTTP web server / application is missing to set the 'Secure' cookie attribute for one or more sent HTTP cookie.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
`The cookie(s):`
`Set-Cookie: XSRF-TOKEN=eyJpdiI6InM0ei81UFBCOENNNWJocHgrcUdHOUE9PSIsInZhbHVlIjoid`
`↪FI2MFRPQmYzY3l6Y3BSQ0p2ZVUyY0U0WW01cUpERVJ4MVhNekZFZkdYbHF4bU1RbW5URjg2bUd6R3F`
`↪0WUZqRnVuaGJhNUF2UElrM2kxRjU5eC9zVkVmeVd6TU4yWEc3RE9qS0hETWFBMHBzWEx1aWluVVphM`
`↪XdRb1FDRW9xa2EiLCJtYWMiOiIzZjMxNTI1ZGQwNWU0MmJkZGU2OGI2YzM3MDg3OTRkNzBlYjg3NDE`
`↪zODJjYmVmMTIyMjkxMzk2ZjQ0MGJhM2FjIiwidGFnIjoiIn0%3D; expires=Thu, 13 Feb 2025`
`↪15:54:44 GMT; Max-Age=***replaced***; path=/; samesite=lax`
`Set-Cookie: gest_ul_session=eyJpdiI6InRvOVlCUlRDZmhRbW0xaE5xV1dRRmc9PSIsInZhbHVl`
`↪IjoiTFBwOGpZOTlJckRYempzaFMvR3QzSkZjM04rK2twaTI4dmVFc0Nxd0dRTVNRTXdNZ2ZLU2tWRn`
`↪JGa1RXb3NBTWkwOW9nbS8wcTFsRWFRV2J6SmE3YUNJODB6ZFBlZXpmSkN3TUpYL0U2bFpZWEIwZ05U`
`↪UW9wNmhETzlRSzAwbjAiLCJtYWMiOiI1MjljZDMwNDliNWE3NTAyNTdiNDljZTJmNDNkOGFkODcxYm`

... continues on next page ...

... continued from previous page ...

```
↪E0MDU4N2U0ZmJjNGRiYzkwMzIzYzkyMThkNTEzIiwidGFnIjoiIn0%3D; expires=Thu, 13 Feb
↪2025 15:54:44 GMT; Max-Age=***replaced***; path=/; httponly; samesite=lax
is/are missing the "Secure" cookie attribute.
```

**Solution:**
**Solution type:** Mitigation
- Set the 'Secure' cookie attribute for any cookies that are sent over a SSL/TLS connection
- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

**Affected Software/OS**
Any web application accessible via a SSL/TLS connection (HTTPS) and at the same time also accessible over a cleartext connection (HTTP).

**Vulnerability Insight**
The flaw exists if a cookie is not using the 'Secure' cookie attribute and is sent over a SSL/TLS connection.
This allows a cookie to be passed to the server by the client over non-secure channels (HTTP) and subsequently allows an attacker to e.g. conduct session hijacking attacks.

**Vulnerability Detection Method**
Checks all cookies sent by the remote HTTP web server / application over a SSL/TLS connection for a missing 'Secure' cookie attribute.
Details: `Missing 'Secure' Cookie Attribute (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.902661
Version used: `2024-09-27T05:05:23Z`

**References**
`url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.5`
`url: https://owasp.org/www-community/controls/SecureCookieAttribute`
`url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0`
`↪02)`

[ return to 172.20.1.55 ]

### 2.17.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565`
`↪)`

... continues on next page ...

... continued from previous page ...

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[ return to 172.20.1.55 ]

## 2.18 172.20.1.57

| | |
|---|---|
| Host scan start | Thu Feb 13 14:04:25 2025 UTC |
| Host scan end | Thu Feb 13 14:29:42 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 135/tcp | Medium |

### 2.18.1 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

**Summary**
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:172.20.1.57[49664]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:172.20.1.57[49664]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:172.20.1.57[49664]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:172.20.1.57[49664]
     Annotation: KeyIso
Port: 49665/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:172.20.1.57[49665]
Port: 49666/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:172.20.1.57[49666]
     Annotation: Windows Event Log
Port: 49667/tcp
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
```

... continues on next page ...

... continued from previous page ...

```
     Endpoint: ncacn_ip_tcp:172.20.1.57[49667]
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:172.20.1.57[49667]
Port: 49668/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:172.20.1.57[49668]
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:172.20.1.57[49668]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:172.20.1.57[49668]
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:172.20.1.57[49668]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:172.20.1.57[49668]
Port: 49670/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:172.20.1.57[49670]
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

**Impact**
An attacker may use this fact to gain more knowledge about the remote host.

**Solution:**
**Solution type:** Mitigation
Filter incoming traffic to this ports.

**Vulnerability Detection Method**
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: 2022-06-03T10:17:07Z

[ return to 172.20.1.57 ]

## 2.19 172.20.1.4

| | |
|---|---|
| Host scan start | Thu Feb 13 08:37:39 2025 UTC |
| Host scan end | Thu Feb 13 12:42:47 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 8080/tcp | Medium |

... (continues) ...

... (continued) ...

| Service (Port) | Threat Level |
|---|---|
| 3820/tcp | Medium |
| 8181/tcp | Medium |
| 80/tcp | Medium |
| 4848/tcp | Medium |
| 22/tcp | Low |

### 2.19.1 Medium 8080/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The following input fields were identified (URL:input name):`
`http://172.20.1.4:8080/kore/templates/ace/login.xhtml;jsessionid=e790b60d583ce0d`
`↪ec957ae278da3:j_idt17:password`

**Impact**
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.108440
Version used: 2023-09-07T05:05:21Z

**References**
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html

[ return to 172.20.1.4 ]

### 2.19.2 Medium 3820/tcp

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

**Summary**
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Server Temporary Key Size: 1024 bits

**Impact**
An attacker might be able to decrypt the SSL/TLS communication offline.

**Solution:**
**Solution type:** Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

**Vulnerability Insight**
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

**Vulnerability Detection Method**
Checks the DHE temporary public key size.
Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.106223

... continues on next page ...

... continued from previous page ...

Version used: 2024-09-30T08:38:05Z

**References**
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html

[ return to 172.20.1.4 ]

### 2.19.3 Medium 8181/tcp

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

**Summary**
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Server Temporary Key Size: 1024 bits

**Impact**
An attacker might be able to decrypt the SSL/TLS communication offline.

**Solution:**
**Solution type:** Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

**Vulnerability Insight**
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

**Vulnerability Detection Method**
Checks the DHE temporary public key size.
Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: 2024-09-30T08:38:05Z

**References**

... continues on next page ...

... continued from previous page ...

```
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html
```

[ return to 172.20.1.4 ]

### 2.19.4 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The following input fields were identified (URL:input name):`
`http://172.20.1.4/kore/templates/ace/login.xhtml;jsessionid=e75e9abf02fe45ea1c79`
`↪631ba00c:j_idt17:password`
`http://172.20.1.4/kore/templates/ace/login.xhtml;jsessionid=e8b55f88667f87c8fd77`
`↪9c0e07f6:j_idt17:password`

**Impact**
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.108440
Version used: 2023-09-07T05:05:21Z

**References**
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html

[ return to 172.20.1.4 ]

### 2.19.5 Medium 4848/tcp

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

**Summary**
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Server Temporary Key Size: 1024 bits

**Impact**
An attacker might be able to decrypt the SSL/TLS communication offline.

**Solution:**
**Solution type:** Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

**Vulnerability Insight**
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

**Vulnerability Detection Method**
Checks the DHE temporary public key size.
Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.106223

... continues on next page ...

... continued from previous page ...

Version used: 2024-09-30T08:38:05Z

**References**
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html

[ return to 172.20.1.4 ]

### 2.19.6 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm(s):
umac-64-etm@openssh.com
umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms

... continues on next page ...

... continued from previous page ...

- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[ return to 172.20.1.4 ]

## 2.20 172.20.1.253

Host scan start Thu Feb 13 09:15:19 2025 UTC
Host scan end Thu Feb 13 09:26:49 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 21/tcp | Medium |

### 2.20.1 Medium 21/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

**Summary**
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Please specify the password.
Anonymous sessions: 331 Please specify the password.

**Impact**
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

**Vulnerability Detection Method**
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2023-12-20T05:05:58Z`

[ return to 172.20.1.253 ]

## 2.21 172.20.1.35

| | |
|---|---|
| Host scan start | Thu Feb 13 07:41:35 2025 UTC |
| Host scan end | Thu Feb 13 09:15:14 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 22/tcp | Low |

### 2.21.1 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↪)`

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s):`
`umac-64-etm@openssh.com`
`umac-64@openssh.com`

... continues on next page ...

... continued from previous page ...

```
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[ return to 172.20.1.35 ]

## 2.22 172.20.1.160

| | |
|---|---|
| Host scan start | Thu Feb 13 12:17:58 2025 UTC |
| Host scan end | Thu Feb 13 12:44:13 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 22/tcp | Low |

### 2.22.1 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**

. . . continues on next page . . .

... continued from previous page ...

```
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4
```

[ return to 172.20.1.160 ]

## 2.23 172.20.1.56

| | |
|---|---|
| Host scan start | Thu Feb 13 12:44:13 2025 UTC |
| Host scan end | Thu Feb 13 13:05:04 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 22/tcp | Low |

### 2.23.1 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm(s):
umac-64-etm@openssh.com
umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**

... continues on next page ...

... continued from previous page ...

Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[ return to 172.20.1.56 ]

## 2.24 172.20.1.10

| | |
|---|---|
| Host scan start | Thu Feb 13 13:44:33 2025 UTC |
| Host scan end | Thu Feb 13 14:04:24 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 22/tcp | Low |

### 2.24.1 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↪)`

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

... continues on next page ...

... continued from previous page ...

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[ return to 172.20.1.10 ]

## 2.25 172.20.1.41

| | |
|---|---|
| Host scan start | Thu Feb 13 15:40:05 2025 UTC |
| Host scan end | Thu Feb 13 16:35:06 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 22/tcp | Low |

### 2.25.1 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↪)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm ↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
. . . continues on next page . . .

... continued from previous page ...

Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[ return to 172.20.1.41 ]

## 2.26 172.20.1.42

| | |
|---|---|
| Host scan start | Thu Feb 13 07:22:48 2025 UTC |
| Host scan end | Thu Feb 13 08:19:43 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 22/tcp | Low |

### 2.26.1 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[ return to 172.20.1.42 ]

## 2.27 172.20.1.14

Host scan start Thu Feb 13 14:42:55 2025 UTC
Host scan end Thu Feb 13 16:24:58 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 22/tcp | Low |

### 2.27.1 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565`

... continues on next page ...

... continued from previous page ...

↪)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm ↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[ return to 172.20.1.14 ]

## 2.28 172.20.1.15

| | |
|---|---|
| Host scan start | Thu Feb 13 15:34:26 2025 UTC |
| Host scan end | Thu Feb 13 15:56:20 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 22/tcp | Low |

### 2.28.1 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm(s):
umac-64-etm@openssh.com
umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm

... continues on next page ...

... continued from previous page ...

Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[ return to 172.20.1.15 ]

## 2.29 172.20.1.7

| | |
|---|---|
| Host scan start | Thu Feb 13 10:48:17 2025 UTC |
| Host scan end | Thu Feb 13 13:44:32 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 22/tcp | Low |

### 2.29.1 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com

... continues on next page ...

... continued from previous page ...

```
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[ return to 172.20.1.7 ]

## 2.30 172.20.1.153

| | |
|---|---|
| Host scan start | Thu Feb 13 07:22:48 2025 UTC |
| Host scan end | Thu Feb 13 08:33:11 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 22/tcp | Low |

### 2.30.1 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm(s):
umac-64-etm@openssh.com
umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**

. . . continues on next page . . .

... continued from previous page ...

```
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4
```

[ return to 172.20.1.153 ]

---

# Scan Report

February 15, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Reseaux_Users_IT_UL". The scan started at Fri Feb 14 11:28:58 2025 UTC and ended at Fri Feb 14 21:34:52 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 192.168.210.57 | 1 | 1 | 0 | 0 | 0 |
| 192.168.210.73 | 4 | 11 | 1 | 0 | 0 |
| 192.168.210.205 | 3 | 14 | 2 | 0 | 0 |
| 192.168.210.244 | 1 | 10 | 0 | 0 | 0 |
| 192.168.210.31 | 0 | 1 | 0 | 0 | 0 |
| Total: 5 | 9 | 37 | 3 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 49 results selected by the filtering described above. Before filtering there were 341 results.

## 1.1 Host Authentications

| Host | Protocol | Result | Port/User |
|---|---|---|---|
| 192.168.210.57 | SMB | Success | Protocol SMB, Port 445, User |

# 2 Results per Host

## 2.1 192.168.210.57

Host scan start Fri Feb 14 11:29:58 2025 UTC
Host scan end Fri Feb 14 12:30:20 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | High |
| 23/tcp | Medium |

### 2.1.1 High 80/tcp

High (CVSS: 9.8)
NVT: Lighttpd < 1.4.35 Multiple Vulnerabilities - Active Check

**Product detection result**
`cpe:/a:lighttpd:lighttpd:1.4.28`
`Detected by Lighttpd Server Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.111079)`

**Summary**
Lighttpd is prone to multiple vulnerabilities.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
`Vulnerable URL: http://192.168.210.57/etc/passwd`

**Impact**
Successful exploitation will allow remote attackers to execute arbitrary SQL commands and remote attackers to read arbitrary files via hostname.

**Solution:**
**Solution type:** VendorFix
Update to version 1.4.35 or later.

**Affected Software/OS**
Lighttpd versions prior to 1.4.35.

**Vulnerability Insight**
The following flaws exist:
- CVE-2014-2323: mod_mysql_vhost module is not properly sanitizing user supplied input passed via the hostname
- CVE-2014-2324: mod_evhost and mod_simple_vhost modules are not properly sanitizing user supplied input via the hostname

**Vulnerability Detection Method**
Sends a crafted HTTP GET request and checks the response.
Details: `Lighttpd < 1.4.35 Multiple Vulnerabilities - Active Check`
OID:1.3.6.1.4.1.25623.1.0.802072
Version used: `2025-01-21T05:37:33Z`

**Product Detection Result**
Product: `cpe:/a:lighttpd:lighttpd:1.4.28`
Method: `Lighttpd Server Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.111079)

**References**

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2014-2323
cve: CVE-2014-2324
url: https://download.lighttpd.net/lighttpd/security/lighttpd_sa_2014_01.txt
url: https://seclists.org/oss-sec/2014/q1/561
url: https://web.archive.org/web/20210122030421/http://www.securityfocus.com/bid
↪/66153
url: https://web.archive.org/web/20210122030421/http://www.securityfocus.com/bid
↪/66157
cert-bund: CB-K14/0300
dfn-cert: DFN-CERT-2014-0311
```

[ return to 192.168.210.57 ]

### 2.1.2 Medium 23/tcp

Medium (CVSS: 4.8)
NVT: Telnet Unencrypted Cleartext Login

**Summary**
The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.

**Solution:**
**Solution type:** Mitigation
Replace Telnet with a protocol like SSH which supports encrypted connections.

**Vulnerability Detection Method**
Details: `Telnet Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108522
Version used: `2023-10-13T05:06:09Z`

[ return to 192.168.210.57 ]

## 2.2 192.168.210.73

| | |
|---|---|
| Host scan start | Fri Feb 14 12:02:28 2025 UTC |
| Host scan end | Fri Feb 14 15:35:38 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| general/tcp | High |
| 80/tcp | Medium |
| general/tcp | Medium |
| 22/tcp | Medium |
| 21/tcp | Medium |
| 23/tcp | Medium |
| 22/tcp | Low |

### 2.2.1 High general/tcp

High (CVSS: 8.1)
NVT: MikroTik RouterOS RCE Vulnerability (CVE-2021-41987)

**Product detection result**
`cpe:/o:mikrotik:routeros:6.47.10`
`Detected by MikroTik RouterOS Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.`
`↪0.810608)`

**Summary**
MikroTik RouterOS is prone to a remote code execution (RCE) vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`Installed version: 6.47.10`
`Fixed version: 6.48.6`

**Solution:**
**Solution type:** VendorFix
Update to version 6.48.6, 6.49.1, 7.1 or later.

**Affected Software/OS**
MikroTik RouterOS versions prior to 6.48.6, 6.49.x prior to 6.49.1 and 7.x prior to 7.1.

**Vulnerability Insight**
In the SCEP Server of RouterOS in certain Mikrotik products, an attacker can trigger a heap-based buffer overflow that leads to remote code execution.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `MikroTik RouterOS RCE Vulnerability (CVE-2021-41987)`
OID:1.3.6.1.4.1.25623.1.0.124040
Version used: `2022-03-30T03:03:44Z`

. . . continues on next page . . .

... continued from previous page ...

**Product Detection Result**
Product: cpe:/o:mikrotik:routeros:6.47.10
Method: MikroTik RouterOS Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.810608)

**References**
cve: CVE-2021-41987
url: https://teamt5.org/en/posts/vulnerability-mikrotik-cve-2021-41987/

High (CVSS: 7.5)
NVT: MikroTik RouterOS < 6.46.7, 6.47.x < 6.48beta40, 7.x < 7.1beta3 DoS Vulnerability

**Product detection result**
cpe:/o:mikrotik:routeros:6.47.10
Detected by MikroTik RouterOS Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.
↪0.810608)

**Summary**
MikroTik RouterOS is prone to a denial of service (DoS) vulnerability in the SMB server.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Installed version: 6.47.10
Fixed version: 6.48beta40

**Solution:**
**Solution type:** VendorFix
- Update to version 6.46.7 (long-term release), 6.48beta40 (testing release), 7.1beta3 (development release) or later
- Disable the SMB server / functionality
Note: Please set an override for this result if the SMB server / functionality is already disabled

**Affected Software/OS**
MikroTik RouterOS versions prior to 6.46.7, 6.47.x prior to 6.48beta40 and 7.x prior to 7.1beta3.

**Vulnerability Insight**
An array index error in MikroTik RouterOS allows an unauthenticated remote attacker to crash the SMB server via modified setup-request packets, aka SUP-12964.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.

... continues on next page ...

... continued from previous page ...

Details: MikroTik RouterOS < 6.46.7, 6.47.x < 6.48beta40, 7.x < 7.1beta3 DoS Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.144572
Version used: 2023-09-06T05:05:19Z

**Product Detection Result**
Product: cpe:/o:mikrotik:routeros:6.47.10
Method: MikroTik RouterOS Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.810608)

**References**
cve: CVE-2020-11881
url: https://github.com/botlabsDev/CVE-2020-11881
url: https://forum.mikrotik.com/viewtopic.php?f=2&t=166137
url: https://mikrotik.com/download/changelogs/long-term-release-tree#show-tab-tr
↪ee_3-id-8d07e91d70a09af6d7c73ecfbe2aa96a
url: https://mikrotik.com/download/changelogs/testing-release-tree#show-tab-tree
↪_2-id-00066a89cafeebda2054b2ca153ef829
url: https://forum.greenbone.net/t/mikrotik-routeros-6-46-7-6-47-3-7-x-dos-vulne
↪rability/14982/11

## High (CVSS: 7.5)
## NVT: MikroTik RouterOS 6.0.0 < 6.48.8, 6.49.x < 6.49.10 DoS Vulnerability

**Product detection result**
cpe:/o:mikrotik:routeros:6.47.10
Detected by MikroTik RouterOS Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.
↪0.810608)

**Summary**
MikroTik RouterOS is prone to a denial of service (DoS) vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Installed version: 6.47.10
Fixed version: 6.48.8

**Solution:**
**Solution type:** VendorFix
Update to version 6.48.8, 6.49.10 or later.

**Affected Software/OS**

... continues on next page ...

... continued from previous page ...

MikroTik RouterOS version 6.0.0 through 6.48.7 and 6.49.x through 6.49.9.

**Vulnerability Insight**
The web server used by MikroTik RouterOS is affected by a heap memory corruption issue. A remote and unauthenticated attacker can corrupt the server's heap memory by sending a crafted HTTP request. As a result, the web interface crashes and is immediately restarted.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `MikroTik RouterOS 6.0.0 < 6.48.8, 6.49.x < 6.49.10 DoS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.150998
Version used: `2023-10-13T05:06:10Z`

**Product Detection Result**
Product: `cpe:/o:mikrotik:routeros:6.47.10`
Method: `MikroTik RouterOS Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.810608)

**References**
`cve: CVE-2023-30800`
`url: https://vulncheck.com/advisories/mikrotik-jsproxy-dos`
`url: https://gist.github.com/j-baines/fdd1e85482838c6299900c1e859071c2`

High (CVSS: 7.2)
NVT: MikroTik RouterOS < 6.49.8 Privilege Escalation Vulnerability

**Product detection result**
`cpe:/o:mikrotik:routeros:6.47.10`
`Detected by MikroTik RouterOS Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.`
`↪0.810608)`

**Summary**
MikroTik RouterOS is prone to a privilege escalation vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`Installed version: 6.47.10`
`Fixed version: 6.49.8`

**Solution:**
**Solution type:** VendorFix
Update to version 6.49.8 or later.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
MikroTik RouterOS prior to version 6.49.8.

**Vulnerability Insight**
A remote and authenticated attacker can escalate privileges from admin to super-admin on the Winbox or HTTP interface. The attacker can abuse this vulnerability to execute arbitrary code on the system.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `MikroTik RouterOS < 6.49.8 Privilege Escalation Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.150774
Version used: `2023-10-13T05:06:10Z`

**Product Detection Result**
Product: `cpe:/o:mikrotik:routeros:6.47.10`
Method: `MikroTik RouterOS Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.810608)

**References**
`cve: CVE-2023-30799`
`url: https://vulncheck.com/advisories/mikrotik-foisted`
`url: https://vulncheck.com/blog/mikrotik-foisted-revisited`

[ return to 192.168.210.73 ]

### 2.2.2 Medium 80/tcp

Medium (CVSS: 6.4)
NVT: MikroTik RouterOS < 6.49.12, 7.x < 7.13.3 DoS Vulnerability (Loop DoS)

**Summary**
MikroTik RouterOS is prone to a denial of service (DoS) vulnerability dubbed 'Loop DoS'.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
Installed version: 6.47.10
Fixed version:     6.49.12
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix

... continues on next page ...

... continued from previous page ...

Update to version 6.49.12, 7.13.3 or later.

**Affected Software/OS**
MikroTik RouterOS versions prior to 6.49.12 and 7.x through 7.13.2.

**Vulnerability Insight**
A vulnerability was found in the MikroTik RouterOS UPD protocol implementation. This issue may allow an unauthenticated attacker to send maliciously crafted packages leading to a denial of service on the targeted system.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `MikroTik RouterOS < 6.49.12, 7.x < 7.13.3 DoS Vulnerability (Loop DoS)`
OID:1.3.6.1.4.1.25623.1.0.103297
Version used: `2024-09-12T07:59:53Z`

**References**
`cve: CVE-2024-2169`
`url: https://mikrotik.com/download/changelogs`
`url: https://forum.mikrotik.com/viewtopic.php?t=206092`
`url: https://kb.cert.org/vuls/id/417980#MikroTik`
`url: https://cispa.de/en/loop-dos`
`url: https://cispa.saarland/group/rossow/Loop-DoS`
`url: https://github.com/cispa/loop-DoS`
`cert-bund: WID-SEC-2024-0672`

[ return to 192.168.210.73 ]

### 2.2.3 Medium general/tcp

Medium (CVSS: 6.5)
NVT: MikroTik RouterOS < 6.48.2 Multiple DoS Vulnerabilities

**Product detection result**
`cpe:/o:mikrotik:routeros:6.47.10`
`Detected by MikroTik RouterOS Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.`
`↪0.810608)`

**Summary**
MikroTik RouterOS is prone to multiple denial of service (DoS) vulnerabilities.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

... continues on next page ...

... continued from previous page ...

Installed version: 6.47.10
Fixed version: 6.48.2

**Solution:**
**Solution type:** VendorFix
Update to version 6.48.2 or later.

**Affected Software/OS**
MikroTik RouterOS all versions below 6.48.2.

**Vulnerability Insight**
The following vulnerabilities exist:
- CVE-2021-36613: The tr069-client process suffers from a memory corruption vulnerability. By sending a crafted packet, an authenticated remote user can crash the tr069-client process due to NULL pointer dereference.
- CVE-2021-36614: The ptp process suffers from a memory corruption vulnerability. By sending a crafted packet, an authenticated remote user can crash the ptp process due to NULL pointer dereference.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: MikroTik RouterOS < 6.48.2 Multiple DoS Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.127012
Version used: 2022-05-23T03:07:35Z

**Product Detection Result**
Product: cpe:/o:mikrotik:routeros:6.47.10
Method: MikroTik RouterOS Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.810608)

**References**
cve: CVE-2021-36613
cve: CVE-2021-36614
url: https://seclists.org/fulldisclosure/2021/Jul/0

Medium (CVSS: 6.5)
NVT: MikroTik RouterOS <= 6.48.6 DoS Vulnerability

**Product detection result**
cpe:/o:mikrotik:routeros:6.47.10
Detected by MikroTik RouterOS Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.
↪0.810608)

**Summary**

... continues on next page ...

... continued from previous page ...

MikroTik RouterOS is prone to a denial of service (DoS) vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`Installed version: 6.47.10`
`Fixed version: None`

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
MikroTik RouterOS version 6.48.3 and prior.

**Vulnerability Insight**
Mikrotik RouterOs suffers from a memory corruption vulnerability in the /nova/bin/detnet process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `MikroTik RouterOS <= 6.48.6 DoS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.146342
Version used: `2022-08-08T10:24:51Z`

**Product Detection Result**
Product: `cpe:/o:mikrotik:routeros:6.47.10`
Method: `MikroTik RouterOS Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.810608)

**References**
`cve: CVE-2020-20231`
`url: https://github.com/cq674350529/pocs_slides/blob/master/advisory/MikroTik/CV`
`↪E-2020-20231/README.md`
`url: https://mikrotik.com/download/changelogs/long-term-release-tree`

Medium (CVSS: 6.5)
NVT: MikroTik RouterOS DoS Vulnerability (CVE-2022-36522)

**Product detection result**
`cpe:/o:mikrotik:routeros:6.47.10`
`Detected by MikroTik RouterOS Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.`

... continues on next page ...

... continued from previous page ...

↪0.810608)

**Summary**
MikroTik RouterOS is prone to a denial of service vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Installed version: 6.47.10
Fixed version: 6.49.6

**Solution:**
**Solution type:** VendorFix
Update to version 6.49.6 or later.

**Affected Software/OS**
MikroTik RouterOS prior to version 6.49.6.

**Vulnerability Insight**
Mikrotik RouterOs was discovered to contain an assertion failure in the component /advanced-tools/nova/bin/netwatch. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: MikroTik RouterOS DoS Vulnerability (CVE-2022-36522)
OID:1.3.6.1.4.1.25623.1.0.124148
Version used: 2023-10-19T05:05:21Z

**Product Detection Result**
Product: cpe:/o:mikrotik:routeros:6.47.10
Method: MikroTik RouterOS Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.810608)

**References**
cve: CVE-2022-36522
url: https://github.com/cq674350529/pocs_slides/blob/master/advisory/MikroTik/CV
↪E-2022-36522/README.md
url: https://seclists.org/fulldisclosure/2021/Jul/0

[ return to 192.168.210.73 ]

### 2.2.4 Medium 22/tcp

Medium (CVSS: 6.4)
NVT: MikroTik RouterOS < 6.49.12, 7.x < 7.13.3 DoS Vulnerability (Loop DoS)

**Summary**
MikroTik RouterOS is prone to a denial of service (DoS) vulnerability dubbed 'Loop DoS'.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
Installed version: 6.47.10
Fixed version:     6.49.12
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 6.49.12, 7.13.3 or later.

**Affected Software/OS**
MikroTik RouterOS versions prior to 6.49.12 and 7.x through 7.13.2.

**Vulnerability Insight**
A vulnerability was found in the MikroTik RouterOS UPD protocol implementation. This issue may allow an unauthenticated attacker to send maliciously crafted packages leading to a denial of service on the targeted system.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `MikroTik RouterOS < 6.49.12, 7.x < 7.13.3 DoS Vulnerability (Loop DoS)`
OID:1.3.6.1.4.1.25623.1.0.103297
Version used: `2024-09-12T07:59:53Z`

**References**
```
cve: CVE-2024-2169
url: https://mikrotik.com/download/changelogs
url: https://forum.mikrotik.com/viewtopic.php?t=206092
url: https://kb.cert.org/vuls/id/417980#MikroTik
url: https://cispa.de/en/loop-dos
url: https://cispa.saarland/group/rossow/Loop-DoS
url: https://github.com/cispa/loop-DoS
cert-bund: WID-SEC-2024-0672
```

Medium (CVSS: 5.3)
NVT: Weak Host Key Algorithm(s) (SSH)

**Product detection result**
... continues on next page ...

... continued from previous page ...

cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)

**Summary**
The remote SSH server is configured to allow / support weak host key algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
-------------------------------------------------------------------------------
---------
ssh-dss            | Digital Signature Algorithm (DSA) / Digital Signature Stand
ard (DSS)
```

**Solution:**
**Solution type:** Mitigation
Disable the reported weak host key algorithm(s).

**Vulnerability Detection Method**
Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: Weak Host Key Algorithm(s) (SSH)
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc8332
url: https://www.rfc-editor.org/rfc/rfc8709
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol

... continues on next page ...

... continued from previous page ...

Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                      | Reason
-----------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

**Impact**
An attacker can quickly break individual connections.

**Solution:**
**Solution type:** Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

**Vulnerability Insight**
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

**Vulnerability Detection Method**
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak encryption algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc

**Solution:**
**Solution type:** Mitigation
Disable the reported weak encryption algorithm(s).

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

**Vulnerability Detection Method**
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms
Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc8758`
`url: https://www.kb.cert.org/vuls/id/958563`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3`

[ return to 192.168.210.73 ]

### 2.2.5 Medium 21/tcp

Medium (CVSS: 6.4)
NVT: MikroTik RouterOS < 6.49.12, 7.x < 7.13.3 DoS Vulnerability (Loop DoS)

**Summary**
MikroTik RouterOS is prone to a denial of service (DoS) vulnerability dubbed 'Loop DoS'.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`Installed version: 6.47.10`

... continues on next page ...

... continued from previous page ...

```
Fixed version:      6.49.12
Installation
path / port:        /
```

**Solution:**
**Solution type:** VendorFix
Update to version 6.49.12, 7.13.3 or later.

**Affected Software/OS**
MikroTik RouterOS versions prior to 6.49.12 and 7.x through 7.13.2.

**Vulnerability Insight**
A vulnerability was found in the MikroTik RouterOS UPD protocol implementation. This issue may allow an unauthenticated attacker to send maliciously crafted packages leading to a denial of service on the targeted system.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `MikroTik RouterOS < 6.49.12, 7.x < 7.13.3 DoS Vulnerability (Loop DoS)`
OID:1.3.6.1.4.1.25623.1.0.103297
Version used: `2024-09-12T07:59:53Z`

**References**
`cve: CVE-2024-2169`
`url: https://mikrotik.com/download/changelogs`
`url: https://forum.mikrotik.com/viewtopic.php?t=206092`
`url: https://kb.cert.org/vuls/id/417980#MikroTik`
`url: https://cispa.de/en/loop-dos`
`url: https://cispa.saarland/group/rossow/Loop-DoS`
`url: https://github.com/cispa/loop-DoS`
`cert-bund: WID-SEC-2024-0672`

## Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

**Summary**
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**

```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Password required for gbvt
```

... continues on next page ...

... continued from previous page ...

```
Anonymous sessions:     331 Password required for anonymous
```

**Impact**
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

**Solution:**
**Solution type:** Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

**Vulnerability Detection Method**
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2023-12-20T05:05:58Z`

[ return to 192.168.210.73 ]

### 2.2.6 Medium 23/tcp

Medium (CVSS: 4.8)
NVT: Telnet Unencrypted Cleartext Login

**Summary**
The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.

**Solution:**
**Solution type:** Mitigation
Replace Telnet with a protocol like SSH which supports encrypted connections.

**Vulnerability Detection Method**
Details: `Telnet Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108522

... continues on next page ...

... continued from previous page ...

Version used: 2023-10-13T05:06:09Z

[ return to 192.168.210.73 ]

### 2.2.7 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm(s):
hmac-md5
The remote SSH server supports the following weak server-to-client MAC algorithm(s):
hmac-md5

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[ return to 192.168.210.73 ]

## 2.3 192.168.210.205

Host scan start Fri Feb 14 12:32:45 2025 UTC
Host scan end Fri Feb 14 17:57:05 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | High |
| 22/tcp | High |
| 443/tcp | Medium |
| 80/tcp | Medium |
| 22/tcp | Medium |
| 23/tcp | Medium |
| 443/tcp | Low |
| 22/tcp | Low |

### 2.3.1 High 443/tcp

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

... continues on next page ...

... continued from previous page ...

'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378

High (CVSS: 7.4)
NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

**Summary**
OpenSSL is prone to a security bypass vulnerability.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.

**Solution:**
**Solution type:** VendorFix
Updates are available. Please see the references for more information.

**Affected Software/OS**
OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h.

**Vulnerability Insight**
OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

**Vulnerability Detection Method**
Send two SSL ChangeCipherSpec request and check the response.
Details: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105042
Version used: 2025-01-17T15:39:18Z

**References**
cve: CVE-2014-0224
url: https://www.openssl.org/news/secadv/20140605.txt
url: http://www.securityfocus.com/bid/67899
cert-bund: WID-SEC-2023-0500
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K15/0384

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0080
cert-bund: CB-K15/0079
cert-bund: CB-K15/0074
cert-bund: CB-K14/1617
cert-bund: CB-K14/1537
cert-bund: CB-K14/1299
cert-bund: CB-K14/1297
cert-bund: CB-K14/1294
cert-bund: CB-K14/1202
cert-bund: CB-K14/1174
cert-bund: CB-K14/1153
cert-bund: CB-K14/0876
cert-bund: CB-K14/0756
cert-bund: CB-K14/0746
cert-bund: CB-K14/0736
cert-bund: CB-K14/0722
cert-bund: CB-K14/0716
cert-bund: CB-K14/0708
cert-bund: CB-K14/0684
cert-bund: CB-K14/0683
cert-bund: CB-K14/0680
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0078
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1364
dfn-cert: DFN-CERT-2014-1357
dfn-cert: DFN-CERT-2014-1350
dfn-cert: DFN-CERT-2014-1265
dfn-cert: DFN-CERT-2014-1209
dfn-cert: DFN-CERT-2014-0917
dfn-cert: DFN-CERT-2014-0789
dfn-cert: DFN-CERT-2014-0778
dfn-cert: DFN-CERT-2014-0768
dfn-cert: DFN-CERT-2014-0752
dfn-cert: DFN-CERT-2014-0747
dfn-cert: DFN-CERT-2014-0738
dfn-cert: DFN-CERT-2014-0715
dfn-cert: DFN-CERT-2014-0714
dfn-cert: DFN-CERT-2014-0709
```

[ return to 192.168.210.205 ]

### 2.3.2 High 22/tcp

High (CVSS: 7.5)
NVT: Deprecated SSH-1 Protocol Detection

**Summary**
The host is running SSH and is providing / accepting one or more deprecated versions of the SSH protocol which have known cryptographic flaws.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The service is providing / accepting the following deprecated versions of the SS
↪H protocol which have known cryptographic flaws:
1.5
```

**Impact**
Successful exploitation could allows remote attackers to bypass security restrictions and to obtain a client's public host key during a connection attempt and use it to open and authenticate an SSH session to another server with the same access.

**Solution:**
**Solution type:** VendorFix
Reconfigure the SSH service to only provide / accept the SSH protocol version SSH-2.

**Affected Software/OS**
Services providing / accepting the SSH protocol version SSH-1 (1.33 and 1.5).

**Vulnerability Detection Method**
Details: `Deprecated SSH-1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.801993
Version used: `2025-01-21T05:37:33Z`

**References**
```
cve: CVE-2001-0361
cve: CVE-2001-0572
cve: CVE-2001-1473
url: http://www.kb.cert.org/vuls/id/684820
url: http://www.securityfocus.com/bid/2344
url: http://xforce.iss.net/xforce/xfdb/6603
cert-bund: CB-K15/1534
dfn-cert: DFN-CERT-2015-1619
```

[ return to 192.168.210.205 ]

### 2.3.3 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security

. . . continues on next page . . .

... continued from previous page ...

Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**

cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Product detection result**
`cpe:/a:ietf:secure_sockets_layer:3.0`
`Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)`

**Summary**
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto
↪col and supports one or more ciphers. Those supported ciphers can be found in
↪the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020
↪67) VT.
```

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**

... continues on next page ...

... continued from previous page ...

All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

**Vulnerability Detection Method**
Check the used SSL protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_sockets_layer:3.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
`cve: CVE-2016-0800`
`cve: CVE-2014-3566`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://drownattack.com/`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: WID-SEC-2023-0431`
`cert-bund: WID-SEC-2023-0427`
`cert-bund: CB-K18/0094`
`cert-bund: CB-K17/1198`
`cert-bund: CB-K17/1196`
`cert-bund: CB-K16/1828`
`cert-bund: CB-K16/1438`
`cert-bund: CB-K16/1384`
`cert-bund: CB-K16/1141`
`cert-bund: CB-K16/1107`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0792`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0597`
`cert-bund: CB-K16/0459`
`cert-bund: CB-K16/0456`
`cert-bund: CB-K16/0433`
`cert-bund: CB-K16/0424`
`cert-bund: CB-K16/0415`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**

... continues on next page ...

... continued from previous page ...

The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
768:RSA:1E:2.5.4.5=#464F433138353257334A58+1.2.840.113549.1.9.2=#5377697463682E7
↪56E69762D6C6F6D652E7467,CN=Switch.univ-lome.tg (Server certificate)
```

**Impact**

Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**

**Solution type:** Mitigation

Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**

SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**

Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.

Details: `SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..`

OID:1.3.6.1.4.1.25623.1.0.150710

Version used: `2021-12-10T12:48:00Z`

**References**

`url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf`

Medium (CVSS: 5.3)

NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 1024 bits

**Summary**

The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 1024 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 1024 bits (public-key-size:public-key-algorithm:serial:issuer):
```

... continues on next page ...

... continued from previous page ...

768:RSA:1E:2.5.4.5=#464F433138353257334A58+1.2.840.113549.1.9.2=#5377697463682E7
↪56E69762D6C6F6D652E7467,CN=Switch.univ-lome.tg (Server certificate)

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 1024 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 1024 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 1024.
↪..
OID:1.3.6.1.4.1.25623.1.0.150711
Version used: 2021-12-10T12:48:00Z

**References**
url: https://docs.microsoft.com/en-us/archive/blogs/pki/rsa-keys-under-1024-bits
↪-are-blocked
url: https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
The certificate of the remote service expired on 2003-10-30 19:47:36.
Certificate details:
fingerprint (SHA-1) | 7CB9ABF574F4F99A85A68B5D2A725715C26C1E69

... continues on next page ...

... continued from previous page ...

| | |
|---|---|
| fingerprint (SHA-256) | 13CD9A8CC3ADA774CCFC41AE70F109A2D7978D233453EA↪A5BF8E4D13CAD9CC76 |
| issued by | 2.5.4.5=#464F433138353257334A58+1.2.840.113549↪.1.9.2=#5377697463682E756E69762D6C6F6D652E7467,CN=Switch.univ-lome.tg |
| public key algorithm | RSA |
| public key size (bits) | 768 |
| serial | 1C |
| signature algorithm | sha1WithRSAEncryption |
| subject | 2.5.4.5=#464F433138353257334A58+1.2.840.113549↪.1.9.2=#5377697463682E756E69762D6C6F6D652E7467,CN=Switch.univ-lome.tg |
| subject alternative names (SAN) | None |
| valid from | 1993-11-01 19:47:36 UTC |
| valid until | 2003-10-30 19:47:36 UTC |

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

**Summary**
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪----------------------------------------------
```

... continues on next page ...

... continued from previous page ...

| | |
|---|---|
| TLSv1.0 | 10 |

**Impact**
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

**Solution:**
**Solution type:** VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

**Affected Software/OS**
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

**Vulnerability Insight**
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

**Vulnerability Detection Method**
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: 2024-09-27T05:05:23Z

**References**
cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego
↪tiation-dos/
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
url: https://www.openwall.com/lists/oss-security/2011/07/08/2
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-0796
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K17/0980
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**

```
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

**Summary**

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

**Impact**

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**

All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)

... continues on next page ...

... continued from previous page ...

- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_sockets_layer:3.0
Method: SSL/TLS: Version Detection
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              2.5.4.5=#464F433138353257334A58+1.2.840.113549.1.9.2=#5377
↪697463682E756E69762D6C6F6D652E7467,CN=Switch.univ-lome.tg
```

... continues on next page ...

... continued from previous page ...

Signature Algorithm: sha1WithRSAEncryption

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: 2021-10-15T11:13:32Z

**References**
url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-
↪sha-1-based-signature-algorithms/

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

**Summary**
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Server Temporary Key Size: 1024 bits

... continues on next page ...

... continued from previous page ...

**Impact**
An attacker might be able to decrypt the SSL/TLS communication offline.

**Solution:**
**Solution type:** Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

**Vulnerability Insight**
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

**Vulnerability Detection Method**
Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2024-09-30T08:38:05Z`

**References**
`url: https://weakdh.org/`
`url: https://weakdh.org/sysadmin.html`

[ return to 192.168.210.205 ]

### 2.3.4 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The following URLs requires Basic Authentication (URL:realm name):`
`http://192.168.210.205/:"level_15_access"`
`http://192.168.210.205/archive:"level_15_access"`

... continues on next page ...

... continued from previous page ...

```
http://192.168.210.205/banner:"level_15_access"
http://192.168.210.205/es:"level_15_access"
http://192.168.210.205/exec:"level_15_access"
http://192.168.210.205/help:"level_15_access"
```

**Impact**
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

**References**
```
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html
```

[ return to 192.168.210.205 ]

### 2.3.5 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak (Small) Public Key Size(s) (SSH)

**Summary**
The remote SSH server uses a weak (too small) public key size.

... continues on next page ...

... continued from previous page ...

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server uses a public RSA key with the following weak (too small) size: 768

**Impact**
A man-in-the-middle attacker can exploit this vulnerability to record the communication to decrypt the session key and even the messages.

**Solution:**
**Solution type:** Mitigation
- <= 1024 bit for RSA based keys:
Install a RSA public key length of 2048 bits or greater, or to switch to more secure key types.

**Vulnerability Insight**
- <= 1024 bit for RSA based keys:
Best practices require that RSA digital signatures be 2048 or more bits long to provide adequate security. Key lengths of 1024 are considered deprecated since 2011.

**Vulnerability Detection Method**
Checks the public key size of the remote SSH server.
Currently weak (too small) key sizes are defined as the following:
- <= 1024 bit for RSA based keys
Details: Weak (Small) Public Key Size(s) (SSH)
OID:1.3.6.1.4.1.25623.1.0.150712
Version used: 2024-11-29T05:05:36Z

**References**
url: https://web.archive.org/web/20220524214031/https://www.linuxminion.com/ssh-server-public-key-too-small/
url: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
url: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)

... continues on next page ...

... continued from previous page ...

**Summary**
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                      | Reason
-----------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

**Impact**
An attacker can quickly break individual connections.

**Solution:**
**Solution type:** Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

**Vulnerability Insight**
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

**Vulnerability Detection Method**
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak encryption algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc

**Solution:**
**Solution type:** Mitigation
Disable the reported weak encryption algorithm(s).

**Vulnerability Insight**
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.

... continues on next page ...

... continued from previous page ...

- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

**Vulnerability Detection Method**
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms
Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc8758`
`url: https://www.kb.cert.org/vuls/id/958563`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3`

[ return to 192.168.210.205 ]

### 2.3.6 Medium 23/tcp

Medium (CVSS: 4.8)
NVT: Telnet Unencrypted Cleartext Login

**Summary**
The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** Mitigation
Replace Telnet with a protocol like SSH which supports encrypted connections.

**Vulnerability Detection Method**
Details: `Telnet Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108522
Version used: `2023-10-13T05:06:09Z`

[ return to 192.168.210.205 ]

### 2.3.7 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)`

**Summary**
This host is prone to an information disclosure vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

**Solution:**
**Solution type:** Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

**Vulnerability Detection Method**
Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ...
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2014-3566
url: https://www.openssl.org/~bodo/ssl-poodle.pdf
url: http://www.securityfocus.com/bid/70574
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin
↪g-ssl-30.html
cert-bund: WID-SEC-2023-0431
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[ return to 192.168.210.205 ]

### 2.3.8 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
The remote SSH server supports the following weak server-to-client MAC algorithm(s):
hmac-md5
hmac-md5-96
hmac-sha1-96

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms

... continues on next page ...

... continued from previous page ...

- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[ return to 192.168.210.205 ]

## 2.4 192.168.210.244

Host scan start Fri Feb 14 12:30:25 2025 UTC
Host scan end Fri Feb 14 17:34:44 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | High |
| 23/tcp | Medium |
| 80/tcp | Medium |
| 443/tcp | Medium |

### 2.4.1 High 443/tcp

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-1378

[ return to 192.168.210.244 ]

### 2.4.2 Medium 23/tcp

Medium (CVSS: 4.8)
NVT: Telnet Unencrypted Cleartext Login

**Summary**
The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.

**Solution:**
**Solution type:** Mitigation
Replace Telnet with a protocol like SSH which supports encrypted connections.

**Vulnerability Detection Method**
Details: Telnet Unencrypted Cleartext Login
OID:1.3.6.1.4.1.25623.1.0.108522
Version used: 2023-10-13T05:06:09Z

[ return to 192.168.210.244 ]

### 2.4.3 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**

```
The following URLs requires Basic Authentication (URL:realm name):
http://192.168.210.244/+CSCOE+:"level_15_access"
http://192.168.210.244/+CSCOT+:"level_15_access"
http://192.168.210.244/+CSCOU+:"level_15_access"
http://192.168.210.244/+webvpn+:"level_15_access"
http://192.168.210.244/:"level_15_access"
http://192.168.210.244/archive:"level_15_access"
http://192.168.210.244/banner:"level_15_access"
http://192.168.210.244/configure/app/landing:"level_15_access"
http://192.168.210.244/configure/app:"level_15_access"
http://192.168.210.244/configure:"level_15_access"
http://192.168.210.244/de:"level_15_access"
http://192.168.210.244/en:"level_15_access"
http://192.168.210.244/es:"level_15_access"
http://192.168.210.244/exec:"level_15_access"
http://192.168.210.244/fr:"level_15_access"
http://192.168.210.244/help:"level_15_access"
http://192.168.210.244/interface/login:"level_15_access"
http://192.168.210.244/interface:"level_15_access"
http://192.168.210.244/it:"level_15_access"
http://192.168.210.244/template:"level_15_access"
http://192.168.210.244/view:"level_15_access"
```

**Impact**

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**

**Solution type:** Workaround

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**

Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'

Details: `Cleartext Transmission of Sensitive Information via HTTP`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.108440
Version used: 2023-09-07T05:05:21Z

**References**
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html

[ return to 192.168.210.244 ]

### 2.4.4 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)

... continues on next page ...

... continued from previous page ...

- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 1024 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 1024 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 1024 bits (public-key-size:public-key-algorithm:serial:issuer):
768:RSA:52:2.5.4.5=#464F433139343757333246+1.2.840.113549.1.9.2=#5377697463682E7
↪56E69762D6C6F6D652E7467,CN=Switch.univ-lome.tg (Server certificate)
```

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation

... continues on next page ...

... continued from previous page ...

Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 1024 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 1024 bit.
Details: `SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 1024. ↪..`
OID:1.3.6.1.4.1.25623.1.0.150711
Version used: `2021-12-10T12:48:00Z`

**References**
`url: https://docs.microsoft.com/en-us/archive/blogs/pki/rsa-keys-under-1024-bits ↪-are-blocked`
`url: https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final`

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The remote SSL/TLS server is using the following certificate(s) with a RSA key w ↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer): 768:RSA:52:2.5.4.5=#464F433139343757333246+1.2.840.113549.1.9.2=#5377697463682E7 ↪56E69762D6C6F6D652E7467,CN=Switch.univ-lome.tg (Server certificate)`

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: `SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: `2021-12-10T12:48:00Z`

**References**
`url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf`

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

**Summary**
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
-------------------------------------------------------------------------------
↪-----------------------------------------------
TLSv1.0          | 10
```

**Impact**
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

**Solution:**
**Solution type:** VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

**Affected Software/OS**
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

**Vulnerability Insight**
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:

... continues on next page ...

... continued from previous page ...

> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

**Vulnerability Detection Method**
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: 2024-09-27T05:05:23Z

**References**
cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego
↪tiation-dos/
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
url: https://www.openwall.com/lists/oss-security/2011/07/08/2
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-0796
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K17/0980
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**

```
The certificate of the remote service expired on 2003-10-30 19:52:25.
Certificate details:
fingerprint (SHA-1)                | EE059C09D634D06C1AB3B7B32B1367BD96403EEF
fingerprint (SHA-256)              | BC339DF15180F248F502645A8B00D235824E298E2B251A
↪4A194D5F009B0DF5AC
issued by                          | 2.5.4.5=#464F433139343757333246+1.2.840.113549
↪.1.9.2=#5377697463682E756E69762D6C6F6D652E7467,CN=Switch.univ-lome.tg
public key algorithm               | RSA
public key size (bits)             | 768
serial                             | 4E
signature algorithm                | sha1WithRSAEncryption
subject                            | 2.5.4.5=#464F433139343757333246+1.2.840.113549
↪.1.9.2=#5377697463682E756E69762D6C6F6D652E7467,CN=Switch.univ-lome.tg
subject alternative names (SAN)    | None
valid from                         | 1993-11-01 19:52:25 UTC
valid until                        | 2003-10-30 19:52:25 UTC
```

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**

```
cpe:/a:ietf:transport_layer_security:1.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

**Summary**

... continues on next page ...

... continued from previous page ...

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

**Impact**

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**

All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**

Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**

Product: `cpe:/a:ietf:transport_layer_security:1.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**

`cve: CVE-2011-3389`
`cve: CVE-2015-0204`

... continues on next page ...

... continued from previous page ...

```
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

**Summary**
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`Server Temporary Key Size: 1024 bits`

**Impact**
An attacker might be able to decrypt the SSL/TLS communication offline.

**Solution:**
**Solution type:** Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

**Vulnerability Insight**
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

**Vulnerability Detection Method**
Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223

... continues on next page ...

... continued from previous page ...

Version used: 2024-09-30T08:38:05Z

**References**
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              2.5.4.5=#464F433139343757333246+1.2.840.113549.1.9.2=#5377
↪697463682E756E69762D6C6F6D652E7467,CN=Switch.univ-lome.tg
Signature Algorithm:  sha1WithRSAEncryption
```

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**

... continues on next page ...

... continued from previous page ...

Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: 2021-10-15T11:13:32Z

**References**
url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

[ return to 192.168.210.244 ]

## 2.5 192.168.210.31

Host scan start Fri Feb 14 12:26:05 2025 UTC
Host scan end Fri Feb 14 15:19:36 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 135/tcp | Medium |

### 2.5.1 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

**Summary**
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:
Port: 49664/tcp
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
Endpoint: ncacn_ip_tcp:192.168.210.31[49664]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : SAM access
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
Endpoint: ncacn_ip_tcp:192.168.210.31[49664]
Annotation: Ngc Pop Key Service
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
Endpoint: ncacn_ip_tcp:192.168.210.31[49664]

... continues on next page ...

... continued from previous page ...

```
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.210.31[49664]
     Annotation: KeyIso
Port: 49665/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.210.31[49665]
Port: 49666/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.210.31[49666]
     Annotation: Event log TCPIP
Port: 49667/tcp
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.210.31[49667]
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.210.31[49667]
Port: 49703/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:192.168.210.31[49703]
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:192.168.210.31[49703]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:192.168.210.31[49703]
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:192.168.210.31[49703]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:192.168.210.31[49703]
Port: 49733/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.210.31[49733]
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

**Impact**
An attacker may use this fact to gain more knowledge about the remote host.

**Solution:**
**Solution type:** Mitigation
Filter incoming traffic to this ports.

**Vulnerability Detection Method**
Details: `DCE/RPC and MSRPC Services Enumeration Reporting`

... continues on next page ...

... continued from previous page ...

| |
|---|
| OID:1.3.6.1.4.1.25623.1.0.10736<br>Version used: 2022-06-03T10:17:07Z |

[ return to 192.168.210.31 ]

---

# Scan Report

February 15, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Réseaux_Users_FSS_UL". The scan started at Sat Feb 15 10:02:27 2025 UTC and ended at . The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 192.168.150.197 | 0 | 1 | 0 | 0 | 0 |
| 192.168.150.175 | 0 | 1 | 0 | 0 | 0 |
| Total: 2 | 0 | 2 | 0 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 2 results selected by the filtering described above. Before filtering there were 83 results.

# 2 Results per Host

## 2.1 192.168.150.197

| | |
|---|---|
| Host scan start | Sat Feb 15 10:03:29 2025 UTC |
| Host scan end | Sat Feb 15 10:25:41 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 135/tcp | Medium |

### 2.1.1 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

**Summary**
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

**Quality of Detection (QoD):** 80%

. . . continues on next page . . .

... continued from previous page ...

**Vulnerability Detection Result**

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.150.197[49664]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:192.168.150.197[49664]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.150.197[49664]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.150.197[49664]
     Annotation: KeyIso
Port: 49665/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.150.197[49665]
Port: 49666/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.150.197[49666]
     Annotation: Windows Event Log
Port: 49667/tcp
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.150.197[49667]
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.150.197[49667]
Port: 49668/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:192.168.150.197[49668]
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:192.168.150.197[49668]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:192.168.150.197[49668]
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:192.168.150.197[49668]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:192.168.150.197[49668]
Port: 49672/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.150.197[49672]
```

... continues on next page ...

... continued from previous page ...

Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.

**Impact**
An attacker may use this fact to gain more knowledge about the remote host.

**Solution:**
**Solution type:** Mitigation
Filter incoming traffic to this ports.

**Vulnerability Detection Method**
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: 2022-06-03T10:17:07Z

[ return to 192.168.150.197 ]

## 2.2 192.168.150.175

Host scan start Sat Feb 15 10:08:12 2025 UTC
Host scan end

| Service (Port) | Threat Level |
|---|---|
| 8686/tcp | Medium |

### 2.2.1 Medium 8686/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The following input fields were identified (URL:input name):
http://192.168.150.175:8686/auth1.html:pwd

**Impact**

... continues on next page ...

... continued from previous page ...

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

**References**
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[ return to 192.168.150.175 ]

# Scan Report

February 13, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Réseaux_Users_FDS_UL". The scan started at Thu Feb 13 07:25:11 2025 UTC and ended at Thu Feb 13 08:18:13 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 192.168.216.47 | 0 | 2 | 0 | 0 | 0 |
| Total: 1 | 0 | 2 | 0 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 2 results selected by the filtering described above. Before filtering there were 37 results.

# 2 Results per Host

## 2.1 192.168.216.47

| | |
|---|---|
| Host scan start | Thu Feb 13 07:26:27 2025 UTC |
| Host scan end | Thu Feb 13 08:18:10 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | Medium |

### 2.1.1 Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Missing 'HttpOnly' Cookie Attribute (HTTP)

**Summary**
The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP cookie.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
`The cookie(s):`

. . . continues on next page . . .

... continued from previous page ...

```
Set-Cookie: COOKIE=ac14013907cec701; PATH=/; MAXAGE=***replaced***; VERSION=1
is/are missing the "HttpOnly" cookie attribute.
```

**Solution:**
**Solution type:** Mitigation
- Set the 'HttpOnly' cookie attribute for any session cookie
- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

**Affected Software/OS**
Any web application with session handling in cookies.

**Vulnerability Insight**
The flaw exists if a session cookie is not using the 'HttpOnly' cookie attribute.
This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

**Vulnerability Detection Method**
Checks all cookies sent by the remote HTTP web server / application for a missing 'HttpOnly' cookie attribute.
Details: `Missing 'HttpOnly' Cookie Attribute (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.105925
Version used: `2024-01-12T16:12:12Z`

**References**
`url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6`
`url: https://owasp.org/www-community/HttpOnly`
`url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0`
`↪02)`

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The following input fields were identified (URL:input name):
http://192.168.216.47/:password
```

**Impact**

... continues on next page ...

... continued from previous page ...

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

**References**
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[ return to 192.168.216.47 ]

# Scan Report

February 15, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP 192.168.224.132". The scan started at Sat Feb 15 09:40:25 2025 UTC and ended at Sat Feb 15 09:47:03 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 192.168.224.132 | 0 | 2 | 1 | 0 | 0 |
| Total: 1 | 0 | 2 | 1 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 3 results selected by the filtering described above. Before filtering there were 14 results.

# 2 Results per Host

## 2.1 192.168.224.132

| | |
|---|---|
| Host scan start | Sat Feb 15 09:41:17 2025 UTC |
| Host scan end | Sat Feb 15 09:47:00 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 22/tcp | Medium |
| 22/tcp | Low |

### 2.1.1 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Host Key Algorithm(s) (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565`
`↪)`

**Summary**

. . . continues on next page . . .

... continued from previous page ...

The remote SSH server is configured to allow / support weak host key algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
-------------------------------------------------------------------------------
↪---------
ssh-dss            | Digital Signature Algorithm (DSA) / Digital Signature Stand
↪ard (DSS)
```

**Solution:**
**Solution type:** Mitigation
Disable the reported weak host key algorithm(s).

**Vulnerability Detection Method**
Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: `Weak Host Key Algorithm(s) (SSH)`
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc8332`
`url: https://www.rfc-editor.org/rfc/rfc8709`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6`

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Product detection result**

```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

**Summary**

... continues on next page ...

... continued from previous page ...

The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm               | Reason
-------------------------------------------------------------------------------
↪---
diffie-hellman-group1-sha1 | Using Oakley Group 2 (a 1024-bit MODP group) and SH
↪A-1
```

**Impact**

An attacker can quickly break individual connections.

**Solution:**

**Solution type:** Mitigation

Disable the reported weak KEX algorithm(s)

- 1024-bit MODP group / prime KEX algorithms:

Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

**Vulnerability Insight**

- 1024-bit MODP group / prime KEX algorithms:

Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

**Vulnerability Detection Method**

Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:

- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key

Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**

Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**

... continues on next page ...

... continued from previous page ...

url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5

[ return to 192.168.224.132 ]

### 2.1.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm(s):
hmac-md5
The remote SSH server supports the following weak server-to-client MAC algorithm(s):
hmac-md5

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[ return to 192.168.224.132 ]

# Scan Report

February 14, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Réseaux_Users_EPL_UL". The scan started at Thu Feb 13 08:30:26 2025 UTC and ended at Fri Feb 14 01:39:11 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 192.168.223.150 | 0 | 1 | 0 | 0 | 0 |
| Total: 1 | 0 | 1 | 0 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains result 1 of the 1 results selected by the filtering above. Before filtering there were 183 results.

# 2 Results per Host

## 2.1 192.168.223.150

| | |
|---|---|
| Host scan start | Thu Feb 13 09:05:56 2025 UTC |
| Host scan end | Fri Feb 14 01:39:03 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | Medium |

### 2.1.1 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The following URLs requires Basic Authentication (URL:realm name):`

... continues on next page ...

... continued from previous page ...

```
http://192.168.223.150/:"TP-LINK Wireless N Access Point WA801N"
http://192.168.223.150/dynaform/css_help.css:"TP-LINK Wireless N Access Point WA
↪801N"
http://192.168.223.150/dynaform/css_main.css:"TP-LINK Wireless N Access Point WA
↪801N"
```

**Impact**
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

**References**
```
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html
```

[ return to 192.168.223.150 ]

# Scan Report

February 14, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Reéseaux_Users_FASEG_PRESIDENCE_UL". The scan started at Thu Feb 13 07:58:43 2025 UTC and ended at Fri Feb 14 11:14:43 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 192.168.228.219 | 3 | 7 | 0 | 0 | 0 |
| 192.168.228.20 | 3 | 7 | 1 | 0 | 0 |
| 192.168.228.227 | 3 | 7 | 1 | 0 | 0 |
| 192.168.228.221 | 3 | 7 | 0 | 0 | 0 |
| 192.168.228.209 | 3 | 7 | 1 | 0 | 0 |
| 192.168.228.46 | 3 | 7 | 1 | 0 | 0 |
| 192.168.228.98 | 3 | 7 | 1 | 0 | 0 |
| 192.168.228.99 | 3 | 7 | 1 | 0 | 0 |
| 192.168.228.101 | 1 | 5 | 1 | 0 | 0 |
| 192.168.228.151 | 0 | 1 | 0 | 0 | 0 |
| 192.168.228.120 | 0 | 1 | 0 | 0 | 0 |
| Total: 11 | 25 | 63 | 7 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 95 results selected by the filtering described above. Before filtering there were 543 results.

# 2 Results per Host

## 2.1 192.168.228.219

| | |
|---|---|
| Host scan start | Thu Feb 13 09:04:53 2025 UTC |
| Host scan end | Thu Feb 13 11:54:23 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | High |
| 443/tcp | High |
| 80/tcp | Medium |
| 443/tcp | Medium |

### 2.1.1 High 80/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          http://192.168.228.219/goform/login
Response(s): Location: http://gbvt1967308930/cscfb8dd5a/goform/login
                       This document has moved to a new <a href="http://gbvt196
↪7308930/cscfb8dd5a/goform/login">location</a>.
URL:          http://192.168.228.219/config/log_off_page.htm
Response(s): Location: http://gbvt134229316/cscfb8dd5a/config/log_off_page.htm
                       This document has moved to a new <a href="http://gbvt134
↪229316/cscfb8dd5a/config/log_off_page.htm">location</a>.
URL:          http://192.168.228.219/
Response(s): Location: http://gbvt1457512254/cscfb8dd5a/
                       This document has moved to a new <a href="http://gbvt145
↪7512254/cscfb8dd5a/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

. . . continues on next page . . .

... continued from previous page ...

**References**
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv
↪er%20HTTP%20Header%20Injection

[ return to 192.168.228.219 ]

### 2.1.2 High 443/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:         https://192.168.228.219/goform/login
Response(s): Location: https://gbvt108288434/cscfb8dd5a/goform/login
                       This document has moved to a new <a href="https://gbvt10
↪8288434/cscfb8dd5a/goform/login">location</a>.
URL:         https://192.168.228.219/config/log_off_page.htm
Response(s): Location: https://gbvt1107265204/cscfb8dd5a/config/log_off_page.htm
                       This document has moved to a new <a href="https://gbvt11
↪07265204/cscfb8dd5a/config/log_off_page.htm">location</a>.
URL:         https://192.168.228.219/
Response(s): Location: https://gbvt104043502/cscfb8dd5a/
                       This document has moved to a new <a href="https://gbvt10
↪4043502/cscfb8dd5a/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**
`cve: CVE-2019-16645`
`url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20server%20HTTP%20Header%20Injection`

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)`

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
```

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: `SSL/TLS: Report Vulnerable Cipher Suites for HTTPS`
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: `2024-09-30T08:38:05Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2016-2183`
`cve: CVE-2016-6329`
`cve: CVE-2020-12872`
`url: https://bettercrypto.org/`
`url: https://mozilla.github.io/server-side-tls/ssl-config-generator/`
`url: https://sweet32.info/`
`cert-bund: WID-SEC-2024-1277`
`cert-bund: WID-SEC-2024-0209`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2022-2226`
`cert-bund: WID-SEC-2022-1955`
`cert-bund: CB-K21/1094`
`cert-bund: CB-K20/1023`
`cert-bund: CB-K20/0321`
`cert-bund: CB-K20/0314`
`cert-bund: CB-K20/0157`
`cert-bund: CB-K19/0618`
`cert-bund: CB-K19/0615`
`cert-bund: CB-K18/0296`
`cert-bund: CB-K17/1980`
`cert-bund: CB-K17/1871`
`cert-bund: CB-K17/1803`
`cert-bund: CB-K17/1753`
`cert-bund: CB-K17/1750`
`cert-bund: CB-K17/1709`
`cert-bund: CB-K17/1558`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 192.168.228.219 ]

### 2.1.3 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**

... continues on next page ...

... continued from previous page ...

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The following input fields were identified (URL:input name):`
`http://192.168.228.219/cscfb8dd5a/config/log_off_page.htm:password$query`

**Impact**
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

**References**
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[ return to 192.168.228.219 ]

### 2.1.4 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**

. . . continues on next page . . .

... continued from previous page ...

These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: `SSL/TLS: Report Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2013-2566`
`cve: CVE-2015-2808`
`cve: CVE-2015-4000`
`url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1`
`↪465_update_6.html`
`url: https://bettercrypto.org/`
`url: https://mozilla.github.io/server-side-tls/ssl-config-generator/`
`cert-bund: CB-K21/0067`
`cert-bund: CB-K19/0812`
`cert-bund: CB-K17/1750`
`cert-bund: CB-K16/1593`
`cert-bund: CB-K16/1552`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0617`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0168`
`cert-bund: CB-K16/0121`
`cert-bund: CB-K16/0090`
`cert-bund: CB-K16/0030`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1591`
`cert-bund: CB-K15/1550`
`cert-bund: CB-K15/1517`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K15/1464`
`cert-bund: CB-K15/1442`
`cert-bund: CB-K15/1334`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:473328CBE11D877AF96174704D60A4A4:OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
↪  (Server certificate)
```

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

**References**
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
The certificate of the remote service expired on 2016-12-20 16:47:02.
Certificate details:

| | |
|---|---|
| fingerprint (SHA-1) | FACE92CADD7801D3EB20D0308C2B6301B1A44FFD |
| fingerprint (SHA-256) | 752C62044107BC02F5232C9E8F2C873A55D1FC8B5355F1 |
| ↪7E5E301D421DAFCD08 | |
| issued by | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| public key algorithm | RSA |
| public key size (bits) | 1024 |
| serial | 473328CBE11D877AF96174704D60A4A4 |
| signature algorithm | sha1WithRSAEncryption |
| subject | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| subject alternative names (SAN) | None |

... continues on next page ...

... continued from previous page ...

| | |
|---|---|
| valid from | 2015-12-21 16:47:02 UTC |
| valid until | 2016-12-20 16:47:02 UTC |

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**
cpe:/a:ietf:transport_layer_security:1.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and ↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c ↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1 ↪.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

... continues on next page ...

... continued from previous page ...

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security:1.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
`cve: CVE-2011-3389`
`cve: CVE-2015-0204`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://datatracker.ietf.org/doc/rfc8996/`
`url: https://vnhacker.blogspot.com/2011/09/beast.html`
`url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1266`
`cert-bund: CB-K15/0850`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

**Impact**
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

. . . continues on next page . . .

... continued from previous page ...

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2015-0204
url: https://freakattack.com
url: http://www.securityfocus.com/bid/71936
url: http://secpod.org/blog/?p=3818
url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac
↪toring-nsa.html
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
Signature Algorithm:  sha1WithRSAEncryption
```

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or

... continues on next page ...

... continued from previous page ...

fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

**References**
`url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/`

[ return to 192.168.228.219 ]

## 2.2 192.168.228.20

Host scan start Thu Feb 13 15:59:12 2025 UTC
Host scan end

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | High |
| 80/tcp | High |
| 443/tcp | Medium |
| 443/tcp | Low |

### 2.2.1 High 443/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          https://192.168.228.20/goform/login
Response(s): Location: https://gbvt334859566/csfec05640/goform/login
                       This document has moved to a new <a href="https://gbvt33
↪4859566/csfec05640/goform/login">location</a>.
URL:          https://192.168.228.20/config/log_off_page.htm
Response(s): Location: https://gbvt67784119/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="https://gbvt67
```

... continues on next page ...

... continued from previous page ...

```
↪784119/csfec05640/config/log_off_page.htm">location</a>.
URL:          https://192.168.228.20/
Response(s): Location: https://gbvt1961135871/csfec05640/
                        This document has moved to a new <a href="https://gbvt19
↪61135871/csfec05640/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**

```
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv
↪er%20HTTP%20Header%20Injection
```

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
`'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:`

... continues on next page ...

... continued from previous page ...

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

**References**
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 192.168.228.20 ]

### 2.2.2 High 80/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          http://192.168.228.20/goform/login
Response(s): Location: http://gbvt546230161/csfec05640/goform/login
                       This document has moved to a new <a href="http://gbvt546
↪230161/csfec05640/goform/login">location</a>.
URL:          http://192.168.228.20/config/log_off_page.htm
Response(s): Location: http://gbvt817762471/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="http://gbvt817
↪762471/csfec05640/config/log_off_page.htm">location</a>.
URL:          http://192.168.228.20/
Response(s): Location: http://gbvt1128833637/csfec05640/
                       This document has moved to a new <a href="http://gbvt112
↪8833637/csfec05640/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

. . . continues on next page . . .

... continued from previous page ...

**References**
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20server%20HTTP%20Header%20Injection

[ return to 192.168.228.20 ]

### 2.2.3 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)

... continues on next page ...

... continued from previous page ...

- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**

Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**References**

cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Summary**
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto
↪col and supports one or more ciphers. Those supported ciphers can be found in
↪the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020
↪67) VT.
```

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**

... continues on next page ...

... continued from previous page ...

All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

**Vulnerability Detection Method**
Check the used SSL protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: `2024-09-27T05:05:23Z`

**References**
`cve: CVE-2016-0800`
`cve: CVE-2014-3566`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://drownattack.com/`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: WID-SEC-2023-0431`
`cert-bund: WID-SEC-2023-0427`
`cert-bund: CB-K18/0094`
`cert-bund: CB-K17/1198`
`cert-bund: CB-K17/1196`
`cert-bund: CB-K16/1828`
`cert-bund: CB-K16/1438`
`cert-bund: CB-K16/1384`
`cert-bund: CB-K16/1141`
`cert-bund: CB-K16/1107`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0792`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0597`
`cert-bund: CB-K16/0459`
`cert-bund: CB-K16/0456`
`cert-bund: CB-K16/0433`
`cert-bund: CB-K16/0424`
`cert-bund: CB-K16/0415`
`cert-bund: CB-K16/0413`
`cert-bund: CB-K16/0374`
`cert-bund: CB-K16/0367`
`cert-bund: CB-K16/0331`
`cert-bund: CB-K16/0329`
`cert-bund: CB-K16/0328`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The remote SSL/TLS server is using the following certificate(s) with a RSA key w`

... continues on next page ...

... continued from previous page ...

ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:62B64D02D42DF27F0FEEBF0E61D9A6A8:OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
(Server certificate)

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

**References**
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
The certificate of the remote service expired on 2014-05-02 14:56:26.
Certificate details:

| | |
|---|---|
| fingerprint (SHA-1) | 06721871E3AB67A0DD72829740EB96BADAE66787 |
| fingerprint (SHA-256) | AC88A3D34CADE4DBCE7ACFE4C196EFC7492EC5869544B4 |
| 1A161199342BEA8234 | |
| issued by | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| public key algorithm | RSA |
| public key size (bits) | 1024 |
| serial | 62B64D02D42DF27F0FEEBF0E61D9A6A8 |
| signature algorithm | md5WithRSAEncryption |

... continues on next page ...

... continued from previous page ...

| | |
|---|---|
| subject | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| subject alternative names (SAN) | None |
| valid from | 2013-05-02 14:56:26 UTC |
| valid until | 2014-05-02 14:56:26 UTC |

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Summary**
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

**Impact**
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.

... continues on next page ...

... continued from previous page ...

- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: `SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)`
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: `2024-09-30T08:38:05Z`

**References**
`cve: CVE-2015-0204`
`url: https://freakattack.com`
`url: http://www.securityfocus.com/bid/71936`
`url: http://secpod.org/blog/?p=3818`
`url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac`
`↪toring-nsa.html`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1266`
`cert-bund: CB-K15/0850`
`cert-bund: CB-K15/0764`
`cert-bund: CB-K15/0720`
`cert-bund: CB-K15/0548`
`cert-bund: CB-K15/0526`
`cert-bund: CB-K15/0509`
`cert-bund: CB-K15/0493`
`cert-bund: CB-K15/0384`
`cert-bund: CB-K15/0365`
`cert-bund: CB-K15/0364`
`cert-bund: CB-K15/0302`
`cert-bund: CB-K15/0192`
`cert-bund: CB-K15/0016`
`dfn-cert: DFN-CERT-2018-1408`
`dfn-cert: DFN-CERT-2016-1372`
`dfn-cert: DFN-CERT-2016-1164`
`dfn-cert: DFN-CERT-2016-0388`
`dfn-cert: DFN-CERT-2015-1853`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)

... continues on next page ...

... continued from previous page ...

- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2024-09-27T05:05:23Z

**References**
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
Signature Algorithm:  md5WithRSAEncryption
```

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

**References**
`url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-↪sha-1-based-signature-algorithms/`

[ return to 192.168.228.20 ]

### 2.2.4 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

**Summary**
This host is prone to an information disclosure vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

**Solution:**
**Solution type:** Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

**Vulnerability Insight**
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

**Vulnerability Detection Method**
Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability . ↪..
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: 2024-09-30T08:38:05Z

**References**
cve: CVE-2014-3566
url: https://www.openssl.org/~bodo/ssl-poodle.pdf
url: http://www.securityfocus.com/bid/70574
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin ↪g-ssl-30.html
cert-bund: WID-SEC-2023-0431
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[ return to 192.168.228.20 ]

## 2.3 192.168.228.227

| | |
|---|---|
| Host scan start | Thu Feb 13 13:31:28 2025 UTC |
| Host scan end | Thu Feb 13 16:39:31 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | High |
| 443/tcp | High |
| 443/tcp | Medium |
| 443/tcp | Low |

### 2.3.1 High 80/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          http://192.168.228.227/goform/login
Response(s): Location: http://gbvt195098296/csfec05640/goform/login
                       This document has moved to a new <a href="http://gbvt195
↪098296/csfec05640/goform/login">location</a>.
URL:          http://192.168.228.227/config/log_off_page.htm
Response(s): Location: http://gbvt10077762/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="http://gbvt100
↪77762/csfec05640/config/log_off_page.htm">location</a>.
```

... continues on next page ...

... continued from previous page ...

```
URL:          http://192.168.228.227/
Response(s): Location: http://gbvt2111977316/csfec05640/
                       This document has moved to a new <a href="http://gbvt211
↪1977316/csfec05640/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**
`cve: CVE-2019-16645`
`url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv`
`↪er%20HTTP%20Header%20Injection`

[ return to 192.168.228.227 ]

### 2.3.2 High 443/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:         https://192.168.228.227/goform/login
Response(s): Location: https://gbvt1377013802/csfec05640/goform/login
                       This document has moved to a new <a href="https://gbvt13
↪77013802/csfec05640/goform/login">location</a>.
URL:         https://192.168.228.227/config/log_off_page.htm
Response(s): Location: https://gbvt1180272588/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="https://gbvt11
↪80272588/csfec05640/config/log_off_page.htm">location</a>.
URL:         https://192.168.228.227/
Response(s): Location: https://gbvt262249254/csfec05640/
                       This document has moved to a new <a href="https://gbvt26
↪2249254/csfec05640/">location</a>.
```

**Impact**

An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**

**Solution type:** WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**

Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**

For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**

Send multiple crafted HTTP POST requests and checks the responses.

Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`

OID:1.3.6.1.4.1.25623.1.0.114133

Version used: `2024-09-25T05:06:11Z`

**References**

```
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv
↪er%20HTTP%20Header%20Injection
```

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

. . . continues on next page . . .

... continued from previous page ...

**References**

cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378

[ return to 192.168.228.227 ]

### 2.3.3 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

... continues on next page ...

... continued from previous page ...

'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Product detection result**

... continues on next page ...

... continued from previous page ...

cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

**Summary**
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

**Vulnerability Detection Method**
Check the used SSL protocols of the services provided by this system.
Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_sockets_layer:3.0
Method: SSL/TLS: Version Detection

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**

cve: CVE-2016-0800
cve: CVE-2014-3566
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://drownattack.com/
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-0431
cert-bund: WID-SEC-2023-0427
cert-bund: CB-K18/0094
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1141
cert-bund: CB-K16/1107
cert-bund: CB-K16/1102
cert-bund: CB-K16/0792
cert-bund: CB-K16/0599
cert-bund: CB-K16/0597
cert-bund: CB-K16/0459
cert-bund: CB-K16/0456
cert-bund: CB-K16/0433
cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:7FD4299093E73CCBDD537B2E0F6B3953:OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
↪  (Server certificate)
```

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation

... continues on next page ...

... continued from previous page ...

Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

**References**
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
The certificate of the remote service expired on 2014-05-02 14:56:13.
Certificate details:

| | |
|---|---|
| fingerprint (SHA-1) | A79038539C8B144999165D11ED81BD21C69A9B1E |
| fingerprint (SHA-256) | FFAB52E8C4DFE97B0573651D86D42F08AD582C792B62A6 |
| ↪10A750E5877A6B7F8A | |
| issued by | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| public key algorithm | RSA |
| public key size (bits) | 1024 |
| serial | 7FD4299093E73CCBDD537B2E0F6B3953 |
| signature algorithm | md5WithRSAEncryption |
| subject | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| subject alternative names (SAN) | None |
| valid from | 2013-05-02 14:56:13 UTC |
| valid until | 2014-05-02 14:56:13 UTC |

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.`
`↪802067)`

**Summary**
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
```

**Impact**

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: `SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)`
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: `2024-09-30T08:38:05Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2015-0204`
`url: https://freakattack.com`
`url: http://www.securityfocus.com/bid/71936`
`url: http://secpod.org/blog/?p=3818`
`url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac`
`↪toring-nsa.html`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1266`
`cert-bund: CB-K15/0850`
`cert-bund: CB-K15/0764`
`cert-bund: CB-K15/0720`
`cert-bund: CB-K15/0548`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**

```
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

**Summary**

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

... continues on next page ...

... continued from previous page ...

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_sockets_layer:3.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
`cve: CVE-2011-3389`
`cve: CVE-2015-0204`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://datatracker.ietf.org/doc/rfc8996/`
`url: https://vnhacker.blogspot.com/2011/09/beast.html`
`url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K18/0799`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
Signature Algorithm:  md5WithRSAEncryption
```

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.105880
Version used: 2021-10-15T11:13:32Z

**References**
url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

[ return to 192.168.228.227 ]

### 2.3.4 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)

**Summary**
This host is prone to an information disclosure vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

**Solution:**
**Solution type:** Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

**Vulnerability Insight**
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

**Vulnerability Detection Method**

... continues on next page ...

... continued from previous page ...

Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability .
↪..
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2014-3566
url: https://www.openssl.org/~bodo/ssl-poodle.pdf
url: http://www.securityfocus.com/bid/70574
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin
↪g-ssl-30.html
cert-bund: WID-SEC-2023-0431
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[ return to 192.168.228.227 ]

## 2.4 192.168.228.221

| | |
|---|---|
| Host scan start | Thu Feb 13 12:41:12 2025 UTC |
| Host scan end | Thu Feb 13 15:41:40 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | High |
| 443/tcp | High |
| 80/tcp | Medium |
| 443/tcp | Medium |

### 2.4.1 High 80/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          http://192.168.228.221/goform/login
Response(s): Location: http://gbvt1534153390/cscfb8dd5a/goform/login
                       This document has moved to a new <a href="http://gbvt153
↪4153390/cscfb8dd5a/goform/login">location</a>.
URL:          http://192.168.228.221/config/log_off_page.htm
Response(s): Location: http://gbvt959341879/cscfb8dd5a/config/log_off_page.htm
                       This document has moved to a new <a href="http://gbvt959
↪341879/cscfb8dd5a/config/log_off_page.htm">location</a>.
URL:          http://192.168.228.221/
Response(s): Location: http://gbvt744460415/cscfb8dd5a/
                       This document has moved to a new <a href="http://gbvt744
↪460415/cscfb8dd5a/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix

. . . continues on next page . . .

... continued from previous page ...

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**
`cve: CVE-2019-16645`
`url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv`
`↪er%20HTTP%20Header%20Injection`

[ return to 192.168.228.221 ]

### 2.4.2 High 443/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          https://192.168.228.221/goform/login
Response(s): Location: https://gbvt2027950684/cscfb8dd5a/goform/login
                       This document has moved to a new <a href="https://gbvt20
↪27950684/cscfb8dd5a/goform/login">location</a>.
URL:          https://192.168.228.221/config/log_off_page.htm
Response(s): Location: https://gbvt1786635030/cscfb8dd5a/config/log_off_page.htm
                       This document has moved to a new <a href="https://gbvt17
```

... continues on next page ...

... continued from previous page ...

```
↪86635030/cscfb8dd5a/config/log_off_page.htm">location</a>.
URL:          https://192.168.228.221/
Response(s): Location: https://gbvt1901655464/cscfb8dd5a/
                        This document has moved to a new <a href="https://gbvt19
↪01655464/cscfb8dd5a/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**

```
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv
↪er%20HTTP%20Header%20Injection
```

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

**Summary**

... continues on next page ...

... continued from previous page ...

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
```

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: `SSL/TLS: Report Vulnerable Cipher Suites for HTTPS`
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: `2024-09-30T08:38:05Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2016-2183`
`cve: CVE-2016-6329`
`cve: CVE-2020-12872`
`url: https://bettercrypto.org/`
`url: https://mozilla.github.io/server-side-tls/ssl-config-generator/`

... continues on next page ...

... continued from previous page ...

```
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 192.168.228.221 ]

### 2.4.3 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The following input fields were identified (URL:input name):`
`http://192.168.228.221/cscfb8dd5a/config/log_off_page.htm:password$query`

**Impact**
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**

... continues on next page ...

... continued from previous page ...

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

**References**
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[ return to 192.168.228.221 ]

### 2.4.4 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.`
`↪802067)`

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
`'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:`
`TLS_RSA_EXPORT_WITH_DES40_CBC_SHA`
`TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5`
`TLS_RSA_EXPORT_WITH_RC4_40_MD5`
`TLS_RSA_WITH_RC4_128_MD5`
`TLS_RSA_WITH_RC4_128_SHA`
`TLS_RSA_WITH_SEED_CBC_SHA`
`'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:`
`TLS_RSA_EXPORT_WITH_DES40_CBC_SHA`

... continues on next page ...

... continued from previous page ...

TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/

... continues on next page ...

... continued from previous page ...

```
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2014-0977

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:50E78F90CF6EE5F1DDB6A4F50A94238F:OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
↪ (Server certificate)

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

**References**
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
cpe:/a:ietf:transport_layer_security

... continues on next page ...

... continued from previous page ...

Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
The certificate of the remote service expired on 2016-12-20 16:47:24.
Certificate details:

| | |
|---|---|
| fingerprint (SHA-1) | 94F93BD002A4F55E6B8C4821DC189576952E0136 |
| fingerprint (SHA-256) | 6EC7D25D2C70E1266277D89EA3DDEB6583D6AD1C0A6B26 ↪64BB6A85AEEAEB781F |
| issued by | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| public key algorithm | RSA |
| public key size (bits) | 1024 |
| serial | 50E78F90CF6EE5F1DDB6A4F50A94238F |
| signature algorithm | sha1WithRSAEncryption |
| subject | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| subject alternative names (SAN) | None |
| valid from | 2015-12-21 16:47:24 UTC |
| valid until | 2016-12-20 16:47:24 UTC |

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

**Impact**
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

. . . continues on next page . . .

... continued from previous page ...

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2015-0204
url: https://freakattack.com
url: http://www.securityfocus.com/bid/71936
url: http://secpod.org/blog/?p=3818
url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac
↪toring-nsa.html
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**
cpe:/a:ietf:transport_layer_security:1.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and ↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c ↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1 ↪.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security:1.0
Method: SSL/TLS: Version Detection
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
```

... continues on next page ...

... continued from previous page ...

Signature Algorithm: sha1WithRSAEncryption

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: 2021-10-15T11:13:32Z

**References**
url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-
↪sha-1-based-signature-algorithms/

[ return to 192.168.228.221 ]

## 2.5 192.168.228.209

Host scan start Thu Feb 13 11:54:24 2025 UTC
Host scan end Thu Feb 13 15:03:36 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | High |
| 80/tcp | High |

... (continues) ...

... (continued) ...

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | Medium |
| 443/tcp | Low |

### 2.5.1 High 443/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          https://192.168.228.209/goform/login
Response(s): Location: https://gbvt161532284/cs8941ddbf/goform/login
                       This document has moved to a new <a href="https://gbvt16
↪1532284/cs8941ddbf/goform/login">location</a>.
URL:          https://192.168.228.209/config/log_off_page.htm
Response(s): Location: https://gbvt1116904374/cs8941ddbf/config/log_off_page.htm
                       This document has moved to a new <a href="https://gbvt11
↪16904374/cs8941ddbf/config/log_off_page.htm">location</a>.
URL:          https://192.168.228.209/
Response(s): Location: https://gbvt59462088/cs8941ddbf/
                       This document has moved to a new <a href="https://gbvt59
↪462088/cs8941ddbf/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**
`cve: CVE-2019-16645`
`url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20server%20HTTP%20Header%20Injection`

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)`

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
```
'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
```

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 192.168.228.209 ]

### 2.5.2 High 80/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          http://192.168.228.209/goform/login
Response(s): Location: http://gbvt716432143/cs8941ddbf/goform/login
                       This document has moved to a new <a href="http://gbvt716
↪432143/cs8941ddbf/goform/login">location</a>.
URL:          http://192.168.228.209/config/log_off_page.htm
Response(s): Location: http://gbvt238195021/cs8941ddbf/config/log_off_page.htm
                       This document has moved to a new <a href="http://gbvt238
↪195021/cs8941ddbf/config/log_off_page.htm">location</a>.
URL:          http://192.168.228.209/
Response(s): Location: http://gbvt1182829843/cs8941ddbf/
                       This document has moved to a new <a href="http://gbvt118
↪2829843/cs8941ddbf/">location</a>.
```

**Impact**

An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**

**Solution type:** WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**

Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**

For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**

Send multiple crafted HTTP POST requests and checks the responses.

Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`

OID:1.3.6.1.4.1.25623.1.0.114133

Version used: `2024-09-25T05:06:11Z`

**References**

```
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv
↪er%20HTTP%20Header%20Injection
```

[ return to 192.168.228.209 ]

### 2.5.3 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium

. . . continues on next page . . .

... continued from previous page ...

- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Product detection result**

```
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

**Summary**

It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto
↪col and supports one or more ciphers. Those supported ciphers can be found in
↪the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020
↪67) VT.
```

**Impact**

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

... continues on next page ...

... continued from previous page ...

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

**Vulnerability Detection Method**
Check the used SSL protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_sockets_layer:3.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
`cve: CVE-2016-0800`
`cve: CVE-2014-3566`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://drownattack.com/`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: WID-SEC-2023-0431`
`cert-bund: WID-SEC-2023-0427`
`cert-bund: CB-K18/0094`
`cert-bund: CB-K17/1198`
`cert-bund: CB-K17/1196`
`cert-bund: CB-K16/1828`
`cert-bund: CB-K16/1438`
`cert-bund: CB-K16/1384`
`cert-bund: CB-K16/1141`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/1107
cert-bund: CB-K16/1102
cert-bund: CB-K16/0792
cert-bund: CB-K16/0599
cert-bund: CB-K16/0597
cert-bund: CB-K16/0459
cert-bund: CB-K16/0456
cert-bund: CB-K16/0433
cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:6D8152B7E4FC5B74D6E6268AA0183AD8:OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
↪ (Server certificate)

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size $<$ 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

**References**
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
The certificate of the remote service expired on 2014-05-02 14:54:42.
Certificate details:

| | |
|---|---|
| fingerprint (SHA-1) | ADBF84FCD06AF2E15BFD59C24FC555783B8C7767 |
| fingerprint (SHA-256) | 7E3A121A8C758561465DC53BF5FC7553B21457CF925E22 ↪6DCC78939EE8D5C4F0 |
| issued by | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| public key algorithm | RSA |
| public key size (bits) | 1024 |
| serial | 6D8152B7E4FC5B74D6E6268AA0183AD8 |
| signature algorithm | md5WithRSAEncryption |
| subject | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| subject alternative names (SAN) | None |
| valid from | 2013-05-02 14:54:42 UTC |
| valid until | 2014-05-02 14:54:42 UTC |

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
. . . continues on next page . . .

... continued from previous page ...

Product: cpe:/a:ietf:secure_sockets_layer:3.0
Method: SSL/TLS: Version Detection
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**

cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Product detection result**

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

**Summary**

This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
```

**Impact**

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: `SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)`
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: `2024-09-30T08:38:05Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2015-0204`
`url: https://freakattack.com`
`url: http://www.securityfocus.com/bid/71936`
`url: http://secpod.org/blog/?p=3818`
`url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac`
`↪toring-nsa.html`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1266`
`cert-bund: CB-K15/0850`
`cert-bund: CB-K15/0764`
`cert-bund: CB-K15/0720`
`cert-bund: CB-K15/0548`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
Signature Algorithm:  md5WithRSAEncryption
```

**Solution:**
**Solution type:** Mitigation

... continues on next page ...

... continued from previous page ...

Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

**References**
`url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/`

[ return to 192.168.228.209 ]

### 2.5.4 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)`

... continues on next page ...

... continued from previous page ...

**Summary**
This host is prone to an information disclosure vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

**Solution:**
**Solution type:** Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

**Vulnerability Insight**
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

**Vulnerability Detection Method**
Evaluate previous collected information about this service.
Details: `SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability .`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: `2024-09-30T08:38:05Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2014-3566`
`url: https://www.openssl.org/~bodo/ssl-poodle.pdf`
`url: http://www.securityfocus.com/bid/70574`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html`
`url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin`
`↪g-ssl-30.html`
`cert-bund: WID-SEC-2023-0431`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[ return to 192.168.228.209 ]

## 2.6 192.168.228.46

| | |
|---|---|
| Host scan start | Thu Feb 13 09:20:37 2025 UTC |
| Host scan end | Thu Feb 13 12:55:21 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | High |
| 80/tcp | High |
| 443/tcp | Medium |
| 443/tcp | Low |

### 2.6.1 High 443/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          https://192.168.228.46/goform/login
Response(s): Location: https://gbvt1412653528/csfec05640/goform/login
                       This document has moved to a new <a href="https://gbvt14
↪12653528/csfec05640/goform/login">location</a>.
URL:          https://192.168.228.46/config/log_off_page.htm
Response(s): Location: https://gbvt1680250393/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="https://gbvt16
↪80250393/csfec05640/config/log_off_page.htm">location</a>.
URL:          https://192.168.228.46/
Response(s): Location: https://gbvt5205177/csfec05640/
                       This document has moved to a new <a href="https://gbvt52
↪05177/csfec05640/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

. . . continues on next page . . .

... continued from previous page ...

**References**
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20server%20HTTP%20Header%20Injection

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

... continues on next page ...

... continued from previous page ...

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 192.168.228.46 ]

### 2.6.2 High 80/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          http://192.168.228.46/goform/login
Response(s): Location: http://gbvt1690103458/csfec05640/goform/login
                       This document has moved to a new <a href="http://gbvt169
↪0103458/csfec05640/goform/login">location</a>.
URL:          http://192.168.228.46/config/log_off_page.htm
Response(s): Location: http://gbvt167153892/csfec05640/config/log_off_page.htm
```

... continues on next page ...

... continued from previous page ...

```
                        This document has moved to a new <a href="http://gbvt167
↪153892/csfec05640/config/log_off_page.htm">location</a>.
URL:          http://192.168.228.46/
Response(s): Location: http://gbvt566889054/csfec05640/
                        This document has moved to a new <a href="http://gbvt566
↪889054/csfec05640/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**

```
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv
↪er%20HTTP%20Header%20Injection
```

[ return to 192.168.228.46 ]

### 2.6.3 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
```

... continues on next page ...

... continued from previous page ...

↪802067)

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**

cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Product detection result**
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

**Summary**
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

**Vulnerability Detection Method**
Check the used SSL protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_sockets_layer:3.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
`cve: CVE-2016-0800`
`cve: CVE-2014-3566`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://drownattack.com/`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: WID-SEC-2023-0431`
`cert-bund: WID-SEC-2023-0427`
`cert-bund: CB-K18/0094`
`cert-bund: CB-K17/1198`
`cert-bund: CB-K17/1196`
`cert-bund: CB-K16/1828`
`cert-bund: CB-K16/1438`
`cert-bund: CB-K16/1384`
`cert-bund: CB-K16/1141`
`cert-bund: CB-K16/1107`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0792`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0597`
`cert-bund: CB-K16/0459`
`cert-bund: CB-K16/0456`
`cert-bund: CB-K16/0433`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:56C41EB1523E862B33188E1995CD9BA3:OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
↪  (Server certificate)
```

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: `SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048. ↪..`
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: `2021-12-10T12:48:00Z`

**References**
`url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf`

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

... continues on next page ...

... continued from previous page ...

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
The certificate of the remote service expired on 2014-05-02 14:57:19.
Certificate details:
fingerprint (SHA-1)                | 6696D12E5AE3F808071A6F322880541AB2A7DE27
fingerprint (SHA-256)              | 0867B511088F08864EA14C88B426EA3DB5E955D85F5C0B
↪25DFB682BB9B18FA28
issued by                          | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
public key algorithm               | RSA
public key size (bits)             | 1024
serial                             | 56C41EB1523E862B33188E1995CD9BA3
signature algorithm                | md5WithRSAEncryption
subject                            | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
subject alternative names (SAN)    | None
valid from                         | 2013-05-02 14:57:19 UTC
valid until                        | 2014-05-02 14:57:19 UTC
```

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Product detection result**

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

... continues on next page ...

... continued from previous page ...

**Summary**
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

**Impact**
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**

cve: CVE-2015-0204
url: https://freakattack.com
url: http://www.securityfocus.com/bid/71936
url: http://secpod.org/blog/?p=3818
url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac
↪toring-nsa.html
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
. . . continues on next page . . .

... continued from previous page ...

Product: cpe:/a:ietf:secure_sockets_layer:3.0
Method: SSL/TLS: Version Detection
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**

cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
Signature Algorithm:  md5WithRSAEncryption
```

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:

... continues on next page ...

... continued from previous page ...

- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

**References**
`url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/`

[ return to 192.168.228.46 ]

### 2.6.4 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)`

**Summary**
This host is prone to an information disclosure vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

**Impact**
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

**Solution:**
**Solution type:** Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

**Vulnerability Insight**
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

**Vulnerability Detection Method**
Evaluate previous collected information about this service.
Details: `SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ..`
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: `2024-09-30T08:38:05Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2014-3566`
`url: https://www.openssl.org/~bodo/ssl-poodle.pdf`
`url: http://www.securityfocus.com/bid/70574`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html`
`url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin`
`g-ssl-30.html`
`cert-bund: WID-SEC-2023-0431`
`cert-bund: CB-K17/1198`
`cert-bund: CB-K17/1196`
`cert-bund: CB-K16/1828`
`cert-bund: CB-K16/1438`
`cert-bund: CB-K16/1384`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0156`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[ return to 192.168.228.46 ]

## 2.7 192.168.228.98

Host scan start Thu Feb 13 08:51:19 2025 UTC
Host scan end Thu Feb 13 12:22:05 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | High |
| 443/tcp | High |
| 443/tcp | Medium |
| 443/tcp | Low |

### 2.7.1 High 80/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
```

... continues on next page ...

... continued from previous page ...

```
URL:          http://192.168.228.98/goform/login
Response(s): Location: http://gbvt1862644721/csfec05640/goform/login
                       This document has moved to a new <a href="http://gbvt186
↪2644721/csfec05640/goform/login">location</a>.
URL:          http://192.168.228.98/config/log_off_page.htm
Response(s): Location: http://gbvt856395143/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="http://gbvt856
↪395143/csfec05640/config/log_off_page.htm">location</a>.
URL:          http://192.168.228.98/
Response(s): Location: http://gbvt989334981/csfec05640/
                       This document has moved to a new <a href="http://gbvt989
↪334981/csfec05640/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**
`cve: CVE-2019-16645`
`url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv`
`↪er%20HTTP%20Header%20Injection`

[ return to 192.168.228.98 ]

### 2.7.2 High 443/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          https://192.168.228.98/goform/login
Response(s): Location: https://gbvt1235629074/csfec05640/goform/login
                       This document has moved to a new <a href="https://gbvt12
↪35629074/csfec05640/goform/login">location</a>.
URL:          https://192.168.228.98/config/log_off_page.htm
Response(s): Location: https://gbvt954974612/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="https://gbvt95
↪4974612/csfec05640/config/log_off_page.htm">location</a>.
URL:          https://192.168.228.98/
Response(s): Location: https://gbvt1814947150/csfec05640/
                       This document has moved to a new <a href="https://gbvt18
↪14947150/csfec05640/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

. . . continues on next page . . .

... continued from previous page ...

**References**
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20server%20HTTP%20Header%20Injection

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

... continues on next page ...

... continued from previous page ...

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 192.168.228.98 ]

### 2.7.3 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Product detection result**
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

**Summary**
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto
↪col and supports one or more ciphers. Those supported ciphers can be found in

... continues on next page ...

... continued from previous page ...

↪the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020
↪67) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

**Vulnerability Detection Method**
Check the used SSL protocols of the services provided by this system.
Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_sockets_layer:3.0
Method: SSL/TLS: Version Detection
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
cve: CVE-2016-0800
cve: CVE-2014-3566
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://drownattack.com/
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-0431
cert-bund: WID-SEC-2023-0427

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K18/0094
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1141
cert-bund: CB-K16/1107
cert-bund: CB-K16/1102
cert-bund: CB-K16/0792
cert-bund: CB-K16/0599
cert-bund: CB-K16/0597
cert-bund: CB-K16/0459
cert-bund: CB-K16/0456
cert-bund: CB-K16/0433
cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

... continues on next page ...

... continued from previous page ...

Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: `SSL/TLS: Report Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2013-2566`
`cve: CVE-2015-2808`
`cve: CVE-2015-4000`
`url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1`
`↪465_update_6.html`
`url: https://bettercrypto.org/`
`url: https://mozilla.github.io/server-side-tls/ssl-config-generator/`
`cert-bund: CB-K21/0067`
`cert-bund: CB-K19/0812`
`cert-bund: CB-K17/1750`
`cert-bund: CB-K16/1593`
`cert-bund: CB-K16/1552`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0617`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0168`
`cert-bund: CB-K16/0121`
`cert-bund: CB-K16/0090`
`cert-bund: CB-K16/0030`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1591`
`cert-bund: CB-K15/1550`
`cert-bund: CB-K15/1517`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:6A91EFCAD910DCBED6601AF44862BB8E:OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
↪  (Server certificate)
```

... continues on next page ...

... continued from previous page ...

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: `SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: `2021-12-10T12:48:00Z`

**References**
`url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf`

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25`
`↪623.1.0.103692)`

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
`The certificate of the remote service expired on 2014-05-02 14:56:42.`
`Certificate details:`

| | |
|---|---|
| fingerprint (SHA-1) | 75ABA59A2211D9B5D0456CC45DAE0E91A85534BC |
| fingerprint (SHA-256) | 46EFD70547D2BB503DC176DD9876091B0512D8966C7D7D4F493825E6D10BE9D2 |
| issued by | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| public key algorithm | RSA |

... continues on next page ...

... continued from previous page ...

| | |
|---|---|
| public key size (bits) | 1024 |
| serial | 6A91EFCAD910DCBED6601AF44862BB8E |
| signature algorithm | md5WithRSAEncryption |
| subject | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| subject alternative names (SAN) | None |
| valid from | 2013-05-02 14:56:42 UTC |
| valid until | 2014-05-02 14:56:42 UTC |

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

... continues on next page ...

... continued from previous page ...

'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

**Impact**
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2015-0204
url: https://freakattack.com
url: http://www.securityfocus.com/bid/71936
url: http://secpod.org/blog/?p=3818
url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac
↪toring-nsa.html
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**
`cpe:/a:ietf:secure_sockets_layer:3.0`
`Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)`

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

... continues on next page ...

... continued from previous page ...

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_sockets_layer:3.0
Method: SSL/TLS: Version Detection
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/

... continues on next page ...

... continued from previous page ...

```
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
Signature Algorithm:  md5WithRSAEncryption
```

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1

... continues on next page ...

... continued from previous page ...

or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

**References**
`url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/`

[ return to 192.168.228.98 ]

### 2.7.4 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)`

**Summary**
This host is prone to an information disclosure vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

**Solution:**
**Solution type:** Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

**Vulnerability Detection Method**
Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability .
↪..
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2014-3566
url: https://www.openssl.org/~bodo/ssl-poodle.pdf
url: http://www.securityfocus.com/bid/70574
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin
↪g-ssl-30.html
cert-bund: WID-SEC-2023-0431
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[ return to 192.168.228.98 ]

## 2.8 192.168.228.99

Host scan start Thu Feb 13 08:51:44 2025 UTC
Host scan end Thu Feb 13 12:23:31 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | High |
| 80/tcp | High |
| 443/tcp | Medium |
| 443/tcp | Low |

### 2.8.1 High 443/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          https://192.168.228.99/goform/login
Response(s): Location: https://gbvt253427644/csfec05640/goform/login
                       This document has moved to a new <a href="https://gbvt25
↪3427644/csfec05640/goform/login">location</a>.
URL:          https://192.168.228.99/config/log_off_page.htm
Response(s): Location: https://gbvt1733899510/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="https://gbvt17
↪33899510/csfec05640/config/log_off_page.htm">location</a>.
URL:          https://192.168.228.99/
Response(s): Location: https://gbvt1623855624/csfec05640/
                       This document has moved to a new <a href="https://gbvt16
↪23855624/csfec05640/">location</a>.
```

... continues on next page ...

... continued from previous page ...

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**
`cve: CVE-2019-16645`
`url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv`
`↪er%20HTTP%20Header%20Injection`

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.`
`↪802067)`

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

... continues on next page ...

... continued from previous page ...

'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 192.168.228.99 ]

### 2.8.2 High 80/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          http://192.168.228.99/goform/login
Response(s): Location: http://gbvt1712793079/csfec05640/goform/login
                       This document has moved to a new <a href="http://gbvt171
↪2793079/csfec05640/goform/login">location</a>.
URL:          http://192.168.228.99/config/log_off_page.htm
Response(s): Location: http://gbvt1390997836/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="http://gbvt139
↪0997836/csfec05640/config/log_off_page.htm">location</a>.
URL:          http://192.168.228.99/
Response(s): Location: http://gbvt335811440/csfec05640/
                       This document has moved to a new <a href="http://gbvt335
↪811440/csfec05640/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**
`cve: CVE-2019-16645`
`url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20server%20HTTP%20Header%20Injection`

[ return to 192.168.228.99 ]

### 2.8.3 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)`

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
```
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
```

... continues on next page ...

... continued from previous page ...

TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Product detection result**
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

... continues on next page ...

... continued from previous page ...

**Summary**
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
`In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto`
`↪col and supports one or more ciphers. Those supported ciphers can be found in`
`↪the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020`
`↪67) VT.`

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

**Vulnerability Detection Method**
Check the used SSL protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_sockets_layer:3.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2016-0800
cve: CVE-2014-3566
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://drownattack.com/
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-0431
cert-bund: WID-SEC-2023-0427
cert-bund: CB-K18/0094
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1141
cert-bund: CB-K16/1107
cert-bund: CB-K16/1102
cert-bund: CB-K16/0792
cert-bund: CB-K16/0599
cert-bund: CB-K16/0597
cert-bund: CB-K16/0459
cert-bund: CB-K16/0456
cert-bund: CB-K16/0433
cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:547FE9AB403D8A6925D21D2612AB4EFB:OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
↪  (Server certificate)
```

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

**References**
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
The certificate of the remote service expired on 2014-05-02 14:56:35.
Certificate details:

| | |
|---|---|
| fingerprint (SHA-1) | 23BDA14D867573D478845078867FAA01134CD487 |
| fingerprint (SHA-256) | 07EEC63A1638B86465927BAD5BF0A8A546C710A30B6559 ↪7A4DF21192562D21D0 |
| issued by | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| public key algorithm | RSA |
| public key size (bits) | 1024 |
| serial | 547FE9AB403D8A6925D21D2612AB4EFB |
| signature algorithm | md5WithRSAEncryption |
| subject | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| subject alternative names (SAN) | None |
| valid from | 2013-05-02 14:56:35 UTC |
| valid until | 2014-05-02 14:56:35 UTC |

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**
`cpe:/a:ietf:secure_sockets_layer:3.0`
`Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)`

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
```
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_sockets_layer:3.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Product detection result**

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

... continues on next page ...

... continued from previous page ...

**Summary**
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

**Impact**
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**

cve: CVE-2015-0204
url: https://freakattack.com
url: http://www.securityfocus.com/bid/71936
url: http://secpod.org/blog/?p=3818
url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac
↪toring-nsa.html
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
Signature Algorithm:  md5WithRSAEncryption
```

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

**References**
```
url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-
↪sha-1-based-signature-algorithms/
```

[ return to 192.168.228.99 ]

### 2.8.4 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)

**Summary**
This host is prone to an information disclosure vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

**Solution:**
**Solution type:** Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

**Vulnerability Insight**
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

**Vulnerability Detection Method**
Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ...
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security

... continues on next page ...

... continued from previous page ...

Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**

cve: CVE-2014-3566
url: https://www.openssl.org/~bodo/ssl-poodle.pdf
url: http://www.securityfocus.com/bid/70574
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin
↪g-ssl-30.html
cert-bund: WID-SEC-2023-0431
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[ return to 192.168.228.99 ]

## 2.9 192.168.228.101

Host scan start Thu Feb 13 12:35:13 2025 UTC
Host scan end

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | High |
| 443/tcp | Medium |
| 443/tcp | Low |

### 2.9.1 High 443/tcp

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
```
'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
```

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: `SSL/TLS: Report Vulnerable Cipher Suites for HTTPS`
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: `2024-09-30T08:38:05Z`

**References**
```
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
```

. . . continues on next page . . .

... continued from previous page ...

```
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 192.168.228.101 ]

### 2.9.2 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Summary**
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto
↪col and supports one or more ciphers. Those supported ciphers can be found in
↪the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020
↪67) VT.
```

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

**Vulnerability Detection Method**
Check the used SSL protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: `2024-09-27T05:05:23Z`

**References**
`cve: CVE-2016-0800`
`cve: CVE-2014-3566`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://drownattack.com/`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters`
`↪-report-2014`
`cert-bund: WID-SEC-2023-0431`
`cert-bund: WID-SEC-2023-0427`
`cert-bund: CB-K18/0094`
`cert-bund: CB-K17/1198`
`cert-bund: CB-K17/1196`
`cert-bund: CB-K16/1828`
`cert-bund: CB-K16/1438`
`cert-bund: CB-K16/1384`
`cert-bund: CB-K16/1141`
`cert-bund: CB-K16/1107`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0792`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0597`
`cert-bund: CB-K16/0459`
`cert-bund: CB-K16/0456`
`cert-bund: CB-K16/0433`
`cert-bund: CB-K16/0424`
`cert-bund: CB-K16/0415`
`cert-bund: CB-K16/0413`
`cert-bund: CB-K16/0374`
`cert-bund: CB-K16/0367`
`cert-bund: CB-K16/0331`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

... continues on next page ...

... continued from previous page ...

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
```

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**References**

```
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
The certificate of the remote service expired on 2014-05-02 14:54:44.
Certificate details:
fingerprint (SHA-1)              | 9339DFF83A624ECE9053059F15A54E021C2992FB
fingerprint (SHA-256)            | C191C076B03A16B15024BB0432589157E99DC36F6C31B3
↪7A80AAC02422716553
issued by                        | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
public key algorithm             | RSA
public key size (bits)           | 1024
serial                           | 7AE6FA572338B56EA5D6E305550583D4
signature algorithm              | md5WithRSAEncryption
subject                          | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
subject alternative names (SAN)  | None
valid from                       | 2013-05-02 14:54:44 UTC
valid until                      | 2014-05-02 14:54:44 UTC
```

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `2024-06-14T05:05:48Z`

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Summary**
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

... continues on next page ...

... continued from previous page ...

'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

**Impact**
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: 2024-09-30T08:38:05Z

**References**
cve: CVE-2015-0204
url: https://freakattack.com
url: http://www.securityfocus.com/bid/71936
url: http://secpod.org/blog/?p=3818
url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac
↪toring-nsa.html
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

**Impact**

... continues on next page ...

... continued from previous page ...

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-09-27T05:05:23Z`

**References**
`cve: CVE-2011-3389`
`cve: CVE-2015-0204`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://datatracker.ietf.org/doc/rfc8996/`
`url: https://vnhacker.blogspot.com/2011/09/beast.html`
`url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1266`
`cert-bund: CB-K15/0850`
`cert-bund: CB-K15/0764`
`cert-bund: CB-K15/0720`
`cert-bund: CB-K15/0548`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

[ return to 192.168.228.101 ]

### 2.9.3 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

**Summary**
This host is prone to an information disclosure vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

**Solution:**
**Solution type:** Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

**Vulnerability Insight**
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

**Vulnerability Detection Method**
Evaluate previous collected information about this service.
Details: `SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ..`
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: `2024-09-30T08:38:05Z`

**References**
`cve: CVE-2014-3566`
`url: https://www.openssl.org/~bodo/ssl-poodle.pdf`
`url: http://www.securityfocus.com/bid/70574`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html`
`url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin g-ssl-30.html`
`cert-bund: WID-SEC-2023-0431`
`cert-bund: CB-K17/1198`
`cert-bund: CB-K17/1196`
`cert-bund: CB-K16/1828`
`cert-bund: CB-K16/1438`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[ return to 192.168.228.101 ]

## 2.10 192.168.228.151

| | |
|---|---|
| Host scan start | Thu Feb 13 08:01:52 2025 UTC |
| Host scan end | Thu Feb 13 08:21:26 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 135/tcp | Medium |

### 2.10.1 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

**Summary**
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

**Quality of Detection (QoD):** 80%

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49664]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49664]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49664]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.228.151[49664]
     Annotation: KeyIso
Port: 49665/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49665]
Port: 49666/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49666]
     Annotation: Windows Event Log
Port: 49667/tcp
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49667]
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49667]
Port: 49669/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49669]
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49669]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49669]
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49669]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49669]
Port: 49671/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.228.151[49671]
```

... continues on next page ...

... continued from previous page ...

```
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

**Impact**
An attacker may use this fact to gain more knowledge about the remote host.

**Solution:**
**Solution type:** Mitigation
Filter incoming traffic to this ports.

**Vulnerability Detection Method**
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: 2022-06-03T10:17:07Z

[ return to 192.168.228.151 ]

## 2.11 192.168.228.120

| | |
|---|---|
| Host scan start | Thu Feb 13 08:01:52 2025 UTC |
| Host scan end | Thu Feb 13 08:21:28 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 135/tcp | Medium |

### 2.11.1 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

**Summary**
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.120[49664]
```

... continues on next page ...

... continued from previous page ...

```
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
      UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49664]
      Annotation: Ngc Pop Key Service
      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49664]
      Annotation: Ngc Pop Key Service
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:192.168.228.120[49664]
      Annotation: KeyIso
Port: 49665/tcp
      UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49665]
Port: 49666/tcp
      UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49666]
      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49666]
Port: 49667/tcp
      UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49667]
      Annotation: Windows Event Log
Port: 49669/tcp
      UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49669]
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49669]
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49669]
      UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49669]
      UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49669]
Port: 49683/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:192.168.228.120[49683]
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

**Impact**

An attacker may use this fact to gain more knowledge about the remote host.

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** Mitigation
Filter incoming traffic to this ports.

**Vulnerability Detection Method**
Details: `DCE/RPC and MSRPC Services Enumeration Reporting`
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: `2022-06-03T10:17:07Z`

[ return to 192.168.228.120 ]

# Scan Report

February 14, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Reéseaux_Users_FASEG_PRESIDENCE_UL". The scan started at Thu Feb 13 07:58:43 2025 UTC and ended at Fri Feb 14 11:14:43 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 192.168.228.219 | 3 | 7 | 0 | 0 | 0 |
| 192.168.228.20 | 3 | 7 | 1 | 0 | 0 |
| 192.168.228.227 | 3 | 7 | 1 | 0 | 0 |
| 192.168.228.221 | 3 | 7 | 0 | 0 | 0 |
| 192.168.228.209 | 3 | 7 | 1 | 0 | 0 |
| 192.168.228.46 | 3 | 7 | 1 | 0 | 0 |
| 192.168.228.98 | 3 | 7 | 1 | 0 | 0 |
| 192.168.228.99 | 3 | 7 | 1 | 0 | 0 |
| 192.168.228.101 | 1 | 5 | 1 | 0 | 0 |
| 192.168.228.151 | 0 | 1 | 0 | 0 | 0 |
| 192.168.228.120 | 0 | 1 | 0 | 0 | 0 |
| Total: 11 | 25 | 63 | 7 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 95 results selected by the filtering described above. Before filtering there were 543 results.

# 2 Results per Host

## 2.1 192.168.228.219

| | |
|---|---|
| Host scan start | Thu Feb 13 09:04:53 2025 UTC |
| Host scan end | Thu Feb 13 11:54:23 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | High |
| 443/tcp | High |
| 80/tcp | Medium |
| 443/tcp | Medium |

### 2.1.1 High 80/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          http://192.168.228.219/goform/login
Response(s): Location: http://gbvt1967308930/cscfb8dd5a/goform/login
                       This document has moved to a new <a href="http://gbvt196
↪7308930/cscfb8dd5a/goform/login">location</a>.
URL:          http://192.168.228.219/config/log_off_page.htm
Response(s): Location: http://gbvt134229316/cscfb8dd5a/config/log_off_page.htm
                       This document has moved to a new <a href="http://gbvt134
↪229316/cscfb8dd5a/config/log_off_page.htm">location</a>.
URL:          http://192.168.228.219/
Response(s): Location: http://gbvt1457512254/cscfb8dd5a/
                       This document has moved to a new <a href="http://gbvt145
↪7512254/cscfb8dd5a/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

. . . continues on next page . . .

... continued from previous page ...

**References**
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv
↪er%20HTTP%20Header%20Injection

[ return to 192.168.228.219 ]

### 2.1.2 High 443/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:         https://192.168.228.219/goform/login
Response(s): Location: https://gbvt108288434/cscfb8dd5a/goform/login
                       This document has moved to a new <a href="https://gbvt10
↪8288434/cscfb8dd5a/goform/login">location</a>.
URL:         https://192.168.228.219/config/log_off_page.htm
Response(s): Location: https://gbvt1107265204/cscfb8dd5a/config/log_off_page.htm
                       This document has moved to a new <a href="https://gbvt11
↪07265204/cscfb8dd5a/config/log_off_page.htm">location</a>.
URL:         https://192.168.228.219/
Response(s): Location: https://gbvt104043502/cscfb8dd5a/
                       This document has moved to a new <a href="https://gbvt10
↪4043502/cscfb8dd5a/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**
`cve: CVE-2019-16645`
`url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20server%20HTTP%20Header%20Injection`

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)`

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
```

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: `SSL/TLS: Report Vulnerable Cipher Suites for HTTPS`
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: `2024-09-30T08:38:05Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2016-2183`
`cve: CVE-2016-6329`
`cve: CVE-2020-12872`
`url: https://bettercrypto.org/`
`url: https://mozilla.github.io/server-side-tls/ssl-config-generator/`
`url: https://sweet32.info/`
`cert-bund: WID-SEC-2024-1277`
`cert-bund: WID-SEC-2024-0209`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2022-2226`
`cert-bund: WID-SEC-2022-1955`
`cert-bund: CB-K21/1094`
`cert-bund: CB-K20/1023`
`cert-bund: CB-K20/0321`
`cert-bund: CB-K20/0314`
`cert-bund: CB-K20/0157`
`cert-bund: CB-K19/0618`
`cert-bund: CB-K19/0615`
`cert-bund: CB-K18/0296`
`cert-bund: CB-K17/1980`
`cert-bund: CB-K17/1871`
`cert-bund: CB-K17/1803`
`cert-bund: CB-K17/1753`
`cert-bund: CB-K17/1750`
`cert-bund: CB-K17/1709`
`cert-bund: CB-K17/1558`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 192.168.228.219 ]

### 2.1.3 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**

... continues on next page ...

... continued from previous page ...

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The following input fields were identified (URL:input name):`
`http://192.168.228.219/cscfb8dd5a/config/log_off_page.htm:password$query`

**Impact**
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

**References**
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[ return to 192.168.228.219 ]

### 2.1.4 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**

. . . continues on next page . . .

... continued from previous page ...

These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: `SSL/TLS: Report Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2013-2566`
`cve: CVE-2015-2808`
`cve: CVE-2015-4000`
`url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1`
`↪465_update_6.html`
`url: https://bettercrypto.org/`
`url: https://mozilla.github.io/server-side-tls/ssl-config-generator/`
`cert-bund: CB-K21/0067`
`cert-bund: CB-K19/0812`
`cert-bund: CB-K17/1750`
`cert-bund: CB-K16/1593`
`cert-bund: CB-K16/1552`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0617`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0168`
`cert-bund: CB-K16/0121`
`cert-bund: CB-K16/0090`
`cert-bund: CB-K16/0030`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1591`
`cert-bund: CB-K15/1550`
`cert-bund: CB-K15/1517`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K15/1464`
`cert-bund: CB-K15/1442`
`cert-bund: CB-K15/1334`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:473328CBE11D877AF96174704D60A4A4:OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
↪  (Server certificate)
```

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

**References**
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
The certificate of the remote service expired on 2016-12-20 16:47:02.
Certificate details:

| | |
|---|---|
| fingerprint (SHA-1) | FACE92CADD7801D3EB20D0308C2B6301B1A44FFD |
| fingerprint (SHA-256) | 752C62044107BC02F5232C9E8F2C873A55D1FC8B5355F1 |
| ↪7E5E301D421DAFCD08 | |
| issued by | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| public key algorithm | RSA |
| public key size (bits) | 1024 |
| serial | 473328CBE11D877AF96174704D60A4A4 |
| signature algorithm | sha1WithRSAEncryption |
| subject | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| subject alternative names (SAN) | None |

... continues on next page ...

... continued from previous page ...

| | |
|---|---|
| valid from | 2015-12-21 16:47:02 UTC |
| valid until | 2016-12-20 16:47:02 UTC |

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**
cpe:/a:ietf:transport_layer_security:1.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and ↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c ↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1 ↪.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

... continues on next page ...

... continued from previous page ...

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security:1.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
`cve: CVE-2011-3389`
`cve: CVE-2015-0204`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://datatracker.ietf.org/doc/rfc8996/`
`url: https://vnhacker.blogspot.com/2011/09/beast.html`
`url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1266`
`cert-bund: CB-K15/0850`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

**Impact**
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

. . . continues on next page . . .

... continued from previous page ...

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2015-0204
url: https://freakattack.com
url: http://www.securityfocus.com/bid/71936
url: http://secpod.org/blog/?p=3818
url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac
↪toring-nsa.html
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
Signature Algorithm:  sha1WithRSAEncryption
```

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or

... continues on next page ...

... continued from previous page ...

fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

**References**
`url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/`

[ return to 192.168.228.219 ]

## 2.2 192.168.228.20

Host scan start Thu Feb 13 15:59:12 2025 UTC
Host scan end

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | High |
| 80/tcp | High |
| 443/tcp | Medium |
| 443/tcp | Low |

### 2.2.1 High 443/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          https://192.168.228.20/goform/login
Response(s): Location: https://gbvt334859566/csfec05640/goform/login
                       This document has moved to a new <a href="https://gbvt33
↪4859566/csfec05640/goform/login">location</a>.
URL:          https://192.168.228.20/config/log_off_page.htm
Response(s): Location: https://gbvt67784119/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="https://gbvt67
```

... continues on next page ...

... continued from previous page ...

```
↪784119/csfec05640/config/log_off_page.htm">location</a>.
URL:          https://192.168.228.20/
Response(s): Location: https://gbvt1961135871/csfec05640/
                        This document has moved to a new <a href="https://gbvt19
↪61135871/csfec05640/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**

```
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv
↪er%20HTTP%20Header%20Injection
```

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
`'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:`

... continues on next page ...

... continued from previous page ...

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

**References**
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 192.168.228.20 ]

### 2.2.2 High 80/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          http://192.168.228.20/goform/login
Response(s): Location: http://gbvt546230161/csfec05640/goform/login
                       This document has moved to a new <a href="http://gbvt546
↪230161/csfec05640/goform/login">location</a>.
URL:          http://192.168.228.20/config/log_off_page.htm
Response(s): Location: http://gbvt817762471/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="http://gbvt817
↪762471/csfec05640/config/log_off_page.htm">location</a>.
URL:          http://192.168.228.20/
Response(s): Location: http://gbvt1128833637/csfec05640/
                       This document has moved to a new <a href="http://gbvt112
↪8833637/csfec05640/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

. . . continues on next page . . .

... continued from previous page ...

**References**
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20server%20HTTP%20Header%20Injection

[ return to 192.168.228.20 ]

### 2.2.3 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)

... continues on next page ...

... continued from previous page ...

- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**

Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**References**

cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Summary**
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto
↪col and supports one or more ciphers. Those supported ciphers can be found in
↪the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020
↪67) VT.
```

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**

... continues on next page ...

... continued from previous page ...

All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

**Vulnerability Detection Method**
Check the used SSL protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: `2024-09-27T05:05:23Z`

**References**
`cve: CVE-2016-0800`
`cve: CVE-2014-3566`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://drownattack.com/`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: WID-SEC-2023-0431`
`cert-bund: WID-SEC-2023-0427`
`cert-bund: CB-K18/0094`
`cert-bund: CB-K17/1198`
`cert-bund: CB-K17/1196`
`cert-bund: CB-K16/1828`
`cert-bund: CB-K16/1438`
`cert-bund: CB-K16/1384`
`cert-bund: CB-K16/1141`
`cert-bund: CB-K16/1107`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0792`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0597`
`cert-bund: CB-K16/0459`
`cert-bund: CB-K16/0456`
`cert-bund: CB-K16/0433`
`cert-bund: CB-K16/0424`
`cert-bund: CB-K16/0415`
`cert-bund: CB-K16/0413`
`cert-bund: CB-K16/0374`
`cert-bund: CB-K16/0367`
`cert-bund: CB-K16/0331`
`cert-bund: CB-K16/0329`
`cert-bund: CB-K16/0328`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The remote SSL/TLS server is using the following certificate(s) with a RSA key w`

... continues on next page ...

... continued from previous page ...

ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:62B64D02D42DF27F0FEEBF0E61D9A6A8:OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
(Server certificate)

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

**References**
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
The certificate of the remote service expired on 2014-05-02 14:56:26.
Certificate details:

| | |
|---|---|
| fingerprint (SHA-1) | 06721871E3AB67A0DD72829740EB96BADAE66787 |
| fingerprint (SHA-256) | AC88A3D34CADE4DBCE7ACFE4C196EFC7492EC5869544B4 |
| 1A161199342BEA8234 | |
| issued by | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| public key algorithm | RSA |
| public key size (bits) | 1024 |
| serial | 62B64D02D42DF27F0FEEBF0E61D9A6A8 |
| signature algorithm | md5WithRSAEncryption |

... continues on next page ...

... continued from previous page ...

| | |
|---|---|
| subject | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| subject alternative names (SAN) | None |
| valid from | 2013-05-02 14:56:26 UTC |
| valid until | 2014-05-02 14:56:26 UTC |

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Summary**
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

**Impact**
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.

... continues on next page ...

... continued from previous page ...

- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: `SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)`
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: `2024-09-30T08:38:05Z`

**References**
`cve: CVE-2015-0204`
`url: https://freakattack.com`
`url: http://www.securityfocus.com/bid/71936`
`url: http://secpod.org/blog/?p=3818`
`url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac`
`↪toring-nsa.html`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1266`
`cert-bund: CB-K15/0850`
`cert-bund: CB-K15/0764`
`cert-bund: CB-K15/0720`
`cert-bund: CB-K15/0548`
`cert-bund: CB-K15/0526`
`cert-bund: CB-K15/0509`
`cert-bund: CB-K15/0493`
`cert-bund: CB-K15/0384`
`cert-bund: CB-K15/0365`
`cert-bund: CB-K15/0364`
`cert-bund: CB-K15/0302`
`cert-bund: CB-K15/0192`
`cert-bund: CB-K15/0016`
`dfn-cert: DFN-CERT-2018-1408`
`dfn-cert: DFN-CERT-2016-1372`
`dfn-cert: DFN-CERT-2016-1164`
`dfn-cert: DFN-CERT-2016-0388`
`dfn-cert: DFN-CERT-2015-1853`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)

... continues on next page ...

... continued from previous page ...

- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2024-09-27T05:05:23Z

**References**
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
Signature Algorithm:  md5WithRSAEncryption
```

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

**References**
`url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-↪sha-1-based-signature-algorithms/`

[ return to 192.168.228.20 ]

### 2.2.4 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

**Summary**
This host is prone to an information disclosure vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

**Solution:**
**Solution type:** Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

**Vulnerability Insight**
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

**Vulnerability Detection Method**
Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability . ↪..
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: 2024-09-30T08:38:05Z

**References**
cve: CVE-2014-3566
url: https://www.openssl.org/~bodo/ssl-poodle.pdf
url: http://www.securityfocus.com/bid/70574
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin ↪g-ssl-30.html
cert-bund: WID-SEC-2023-0431
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[ return to 192.168.228.20 ]

## 2.3 192.168.228.227

| | |
|---|---|
| Host scan start | Thu Feb 13 13:31:28 2025 UTC |
| Host scan end | Thu Feb 13 16:39:31 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | High |
| 443/tcp | High |
| 443/tcp | Medium |
| 443/tcp | Low |

### 2.3.1 High 80/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          http://192.168.228.227/goform/login
Response(s): Location: http://gbvt195098296/csfec05640/goform/login
                       This document has moved to a new <a href="http://gbvt195
↪098296/csfec05640/goform/login">location</a>.
URL:          http://192.168.228.227/config/log_off_page.htm
Response(s): Location: http://gbvt10077762/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="http://gbvt100
↪77762/csfec05640/config/log_off_page.htm">location</a>.
```

... continues on next page ...

... continued from previous page ...

```
URL:          http://192.168.228.227/
Response(s): Location: http://gbvt2111977316/csfec05640/
                       This document has moved to a new <a href="http://gbvt211
↪1977316/csfec05640/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**
`cve: CVE-2019-16645`
`url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv`
`↪er%20HTTP%20Header%20Injection`

[ return to 192.168.228.227 ]

### 2.3.2 High 443/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:         https://192.168.228.227/goform/login
Response(s): Location: https://gbvt1377013802/csfec05640/goform/login
                       This document has moved to a new <a href="https://gbvt13
↪77013802/csfec05640/goform/login">location</a>.
URL:         https://192.168.228.227/config/log_off_page.htm
Response(s): Location: https://gbvt1180272588/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="https://gbvt11
↪80272588/csfec05640/config/log_off_page.htm">location</a>.
URL:         https://192.168.228.227/
Response(s): Location: https://gbvt262249254/csfec05640/
                       This document has moved to a new <a href="https://gbvt26
↪2249254/csfec05640/">location</a>.
```

**Impact**

An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**

**Solution type:** WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**

Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**

For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**

Send multiple crafted HTTP POST requests and checks the responses.

Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`

OID:1.3.6.1.4.1.25623.1.0.114133

Version used: `2024-09-25T05:06:11Z`

**References**

```
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv
↪er%20HTTP%20Header%20Injection
```

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

. . . continues on next page . . .

... continued from previous page ...

**References**

cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378

[ return to 192.168.228.227 ]

### 2.3.3 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

... continues on next page ...

... continued from previous page ...

'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Product detection result**

... continues on next page ...

... continued from previous page ...

cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

**Summary**
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

**Vulnerability Detection Method**
Check the used SSL protocols of the services provided by this system.
Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_sockets_layer:3.0
Method: SSL/TLS: Version Detection

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**

cve: CVE-2016-0800
cve: CVE-2014-3566
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://drownattack.com/
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-0431
cert-bund: WID-SEC-2023-0427
cert-bund: CB-K18/0094
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1141
cert-bund: CB-K16/1107
cert-bund: CB-K16/1102
cert-bund: CB-K16/0792
cert-bund: CB-K16/0599
cert-bund: CB-K16/0597
cert-bund: CB-K16/0459
cert-bund: CB-K16/0456
cert-bund: CB-K16/0433
cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:7FD4299093E73CCBDD537B2E0F6B3953:OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
↪  (Server certificate)
```

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation

... continues on next page ...

... continued from previous page ...

Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

**References**
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
The certificate of the remote service expired on 2014-05-02 14:56:13.
Certificate details:

| | |
|---|---|
| fingerprint (SHA-1) | A79038539C8B144999165D11ED81BD21C69A9B1E |
| fingerprint (SHA-256) | FFAB52E8C4DFE97B0573651D86D42F08AD582C792B62A6 |
| ↪10A750E5877A6B7F8A | |
| issued by | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| public key algorithm | RSA |
| public key size (bits) | 1024 |
| serial | 7FD4299093E73CCBDD537B2E0F6B3953 |
| signature algorithm | md5WithRSAEncryption |
| subject | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| subject alternative names (SAN) | None |
| valid from | 2013-05-02 14:56:13 UTC |
| valid until | 2014-05-02 14:56:13 UTC |

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.`
`↪802067)`

**Summary**
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
```

**Impact**

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: `SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)`
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: `2024-09-30T08:38:05Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2015-0204`
`url: https://freakattack.com`
`url: http://www.securityfocus.com/bid/71936`
`url: http://secpod.org/blog/?p=3818`
`url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac`
`↪toring-nsa.html`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1266`
`cert-bund: CB-K15/0850`
`cert-bund: CB-K15/0764`
`cert-bund: CB-K15/0720`
`cert-bund: CB-K15/0548`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**

```
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

**Summary**

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

... continues on next page ...

... continued from previous page ...

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_sockets_layer:3.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
`cve: CVE-2011-3389`
`cve: CVE-2015-0204`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://datatracker.ietf.org/doc/rfc8996/`
`url: https://vnhacker.blogspot.com/2011/09/beast.html`
`url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K18/0799`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
Signature Algorithm:  md5WithRSAEncryption
```

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.105880
Version used: 2021-10-15T11:13:32Z

**References**
url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

[ return to 192.168.228.227 ]

### 2.3.4 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)

**Summary**
This host is prone to an information disclosure vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

**Solution:**
**Solution type:** Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

**Vulnerability Insight**
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

**Vulnerability Detection Method**

... continues on next page ...

... continued from previous page ...

Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability .
↪..
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2014-3566
url: https://www.openssl.org/~bodo/ssl-poodle.pdf
url: http://www.securityfocus.com/bid/70574
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin
↪g-ssl-30.html
cert-bund: WID-SEC-2023-0431
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[ return to 192.168.228.227 ]

## 2.4 192.168.228.221

| | |
|---|---|
| Host scan start | Thu Feb 13 12:41:12 2025 UTC |
| Host scan end | Thu Feb 13 15:41:40 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | High |
| 443/tcp | High |
| 80/tcp | Medium |
| 443/tcp | Medium |

### 2.4.1 High 80/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          http://192.168.228.221/goform/login
Response(s): Location: http://gbvt1534153390/cscfb8dd5a/goform/login
                       This document has moved to a new <a href="http://gbvt153
↪4153390/cscfb8dd5a/goform/login">location</a>.
URL:          http://192.168.228.221/config/log_off_page.htm
Response(s): Location: http://gbvt959341879/cscfb8dd5a/config/log_off_page.htm
                       This document has moved to a new <a href="http://gbvt959
↪341879/cscfb8dd5a/config/log_off_page.htm">location</a>.
URL:          http://192.168.228.221/
Response(s): Location: http://gbvt744460415/cscfb8dd5a/
                       This document has moved to a new <a href="http://gbvt744
↪460415/cscfb8dd5a/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix

. . . continues on next page . . .

... continued from previous page ...

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**
`cve: CVE-2019-16645`
`url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv`
`↪er%20HTTP%20Header%20Injection`

[ return to 192.168.228.221 ]

### 2.4.2 High 443/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          https://192.168.228.221/goform/login
Response(s): Location: https://gbvt2027950684/cscfb8dd5a/goform/login
                       This document has moved to a new <a href="https://gbvt20
↪27950684/cscfb8dd5a/goform/login">location</a>.
URL:          https://192.168.228.221/config/log_off_page.htm
Response(s): Location: https://gbvt1786635030/cscfb8dd5a/config/log_off_page.htm
                       This document has moved to a new <a href="https://gbvt17
```

... continues on next page ...

... continued from previous page ...

```
↪86635030/cscfb8dd5a/config/log_off_page.htm">location</a>.
URL:          https://192.168.228.221/
Response(s): Location: https://gbvt1901655464/cscfb8dd5a/
                        This document has moved to a new <a href="https://gbvt19
↪01655464/cscfb8dd5a/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**

```
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv
↪er%20HTTP%20Header%20Injection
```

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

**Summary**

... continues on next page ...

... continued from previous page ...

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
```

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: `SSL/TLS: Report Vulnerable Cipher Suites for HTTPS`
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: `2024-09-30T08:38:05Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2016-2183`
`cve: CVE-2016-6329`
`cve: CVE-2020-12872`
`url: https://bettercrypto.org/`
`url: https://mozilla.github.io/server-side-tls/ssl-config-generator/`

... continues on next page ...

... continued from previous page ...

```
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 192.168.228.221 ]

### 2.4.3 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The following input fields were identified (URL:input name):`
`http://192.168.228.221/cscfb8dd5a/config/log_off_page.htm:password$query`

**Impact**
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**

... continues on next page ...

... continued from previous page ...

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

**References**
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[ return to 192.168.228.221 ]

### 2.4.4 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.`
`↪802067)`

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
`'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:`
`TLS_RSA_EXPORT_WITH_DES40_CBC_SHA`
`TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5`
`TLS_RSA_EXPORT_WITH_RC4_40_MD5`
`TLS_RSA_WITH_RC4_128_MD5`
`TLS_RSA_WITH_RC4_128_SHA`
`TLS_RSA_WITH_SEED_CBC_SHA`
`'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:`
`TLS_RSA_EXPORT_WITH_DES40_CBC_SHA`

... continues on next page ...

... continued from previous page ...

TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/

... continues on next page ...

... continued from previous page ...

```
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2014-0977

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:50E78F90CF6EE5F1DDB6A4F50A94238F:OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
↪ (Server certificate)

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

**References**
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
cpe:/a:ietf:transport_layer_security

... continues on next page ...

... continued from previous page ...

Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
The certificate of the remote service expired on 2016-12-20 16:47:24.
Certificate details:

| | |
|---|---|
| fingerprint (SHA-1) | 94F93BD002A4F55E6B8C4821DC189576952E0136 |
| fingerprint (SHA-256) | 6EC7D25D2C70E1266277D89EA3DDEB6583D6AD1C0A6B26 ↪64BB6A85AEEAEB781F |
| issued by | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| public key algorithm | RSA |
| public key size (bits) | 1024 |
| serial | 50E78F90CF6EE5F1DDB6A4F50A94238F |
| signature algorithm | sha1WithRSAEncryption |
| subject | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| subject alternative names (SAN) | None |
| valid from | 2015-12-21 16:47:24 UTC |
| valid until | 2016-12-20 16:47:24 UTC |

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

**Impact**
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

. . . continues on next page . . .

... continued from previous page ...

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2015-0204
url: https://freakattack.com
url: http://www.securityfocus.com/bid/71936
url: http://secpod.org/blog/?p=3818
url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac
↪toring-nsa.html
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**
cpe:/a:ietf:transport_layer_security:1.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and ↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c ↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1 ↪.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security:1.0
Method: SSL/TLS: Version Detection
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
```

... continues on next page ...

... continued from previous page ...

Signature Algorithm: sha1WithRSAEncryption

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: 2021-10-15T11:13:32Z

**References**
url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-
↪sha-1-based-signature-algorithms/

[ return to 192.168.228.221 ]

## 2.5 192.168.228.209

Host scan start Thu Feb 13 11:54:24 2025 UTC
Host scan end Thu Feb 13 15:03:36 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | High |
| 80/tcp | High |

... (continues) ...

... (continued) ...

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | Medium |
| 443/tcp | Low |

### 2.5.1 High 443/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          https://192.168.228.209/goform/login
Response(s): Location: https://gbvt161532284/cs8941ddbf/goform/login
                       This document has moved to a new <a href="https://gbvt16
↪1532284/cs8941ddbf/goform/login">location</a>.
URL:          https://192.168.228.209/config/log_off_page.htm
Response(s): Location: https://gbvt1116904374/cs8941ddbf/config/log_off_page.htm
                       This document has moved to a new <a href="https://gbvt11
↪16904374/cs8941ddbf/config/log_off_page.htm">location</a>.
URL:          https://192.168.228.209/
Response(s): Location: https://gbvt59462088/cs8941ddbf/
                       This document has moved to a new <a href="https://gbvt59
↪462088/cs8941ddbf/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**
`cve: CVE-2019-16645`
`url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20server%20HTTP%20Header%20Injection`

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)`

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
```
'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
```

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 192.168.228.209 ]

### 2.5.2 High 80/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          http://192.168.228.209/goform/login
Response(s): Location: http://gbvt716432143/cs8941ddbf/goform/login
                       This document has moved to a new <a href="http://gbvt716
↪432143/cs8941ddbf/goform/login">location</a>.
URL:          http://192.168.228.209/config/log_off_page.htm
Response(s): Location: http://gbvt238195021/cs8941ddbf/config/log_off_page.htm
                       This document has moved to a new <a href="http://gbvt238
↪195021/cs8941ddbf/config/log_off_page.htm">location</a>.
URL:          http://192.168.228.209/
Response(s): Location: http://gbvt1182829843/cs8941ddbf/
                       This document has moved to a new <a href="http://gbvt118
↪2829843/cs8941ddbf/">location</a>.
```

**Impact**

An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**

**Solution type:** WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**

Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**

For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**

Send multiple crafted HTTP POST requests and checks the responses.

Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`

OID:1.3.6.1.4.1.25623.1.0.114133

Version used: `2024-09-25T05:06:11Z`

**References**

```
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv
↪er%20HTTP%20Header%20Injection
```

[ return to 192.168.228.209 ]

### 2.5.3 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium

. . . continues on next page . . .

... continued from previous page ...

- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Product detection result**

```
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

**Summary**

It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto
↪col and supports one or more ciphers. Those supported ciphers can be found in
↪the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020
↪67) VT.
```

**Impact**

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

... continues on next page ...

... continued from previous page ...

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

**Vulnerability Detection Method**
Check the used SSL protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_sockets_layer:3.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
`cve: CVE-2016-0800`
`cve: CVE-2014-3566`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://drownattack.com/`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: WID-SEC-2023-0431`
`cert-bund: WID-SEC-2023-0427`
`cert-bund: CB-K18/0094`
`cert-bund: CB-K17/1198`
`cert-bund: CB-K17/1196`
`cert-bund: CB-K16/1828`
`cert-bund: CB-K16/1438`
`cert-bund: CB-K16/1384`
`cert-bund: CB-K16/1141`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/1107
cert-bund: CB-K16/1102
cert-bund: CB-K16/0792
cert-bund: CB-K16/0599
cert-bund: CB-K16/0597
cert-bund: CB-K16/0459
cert-bund: CB-K16/0456
cert-bund: CB-K16/0433
cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:6D8152B7E4FC5B74D6E6268AA0183AD8:OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
↪ (Server certificate)

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size $<$ 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

**References**
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
The certificate of the remote service expired on 2014-05-02 14:54:42.
Certificate details:

| | |
|---|---|
| fingerprint (SHA-1) | ADBF84FCD06AF2E15BFD59C24FC555783B8C7767 |
| fingerprint (SHA-256) | 7E3A121A8C758561465DC53BF5FC7553B21457CF925E22 ↪6DCC78939EE8D5C4F0 |
| issued by | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| public key algorithm | RSA |
| public key size (bits) | 1024 |
| serial | 6D8152B7E4FC5B74D6E6268AA0183AD8 |
| signature algorithm | md5WithRSAEncryption |
| subject | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| subject alternative names (SAN) | None |
| valid from | 2013-05-02 14:54:42 UTC |
| valid until | 2014-05-02 14:54:42 UTC |

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
. . . continues on next page . . .

... continued from previous page ...

Product: cpe:/a:ietf:secure_sockets_layer:3.0
Method: SSL/TLS: Version Detection
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**

cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Product detection result**

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

**Summary**

This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
```

**Impact**

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: `SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)`
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: `2024-09-30T08:38:05Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2015-0204`
`url: https://freakattack.com`
`url: http://www.securityfocus.com/bid/71936`
`url: http://secpod.org/blog/?p=3818`
`url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac`
`↪toring-nsa.html`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1266`
`cert-bund: CB-K15/0850`
`cert-bund: CB-K15/0764`
`cert-bund: CB-K15/0720`
`cert-bund: CB-K15/0548`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
Signature Algorithm:  md5WithRSAEncryption
```

**Solution:**
**Solution type:** Mitigation

... continues on next page ...

... continued from previous page ...

Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

**References**
`url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/`

[ return to 192.168.228.209 ]

### 2.5.4 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)`

... continues on next page ...

... continued from previous page ...

**Summary**
This host is prone to an information disclosure vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

**Solution:**
**Solution type:** Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

**Vulnerability Insight**
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

**Vulnerability Detection Method**
Evaluate previous collected information about this service.
Details: `SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability .`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: `2024-09-30T08:38:05Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2014-3566`
`url: https://www.openssl.org/~bodo/ssl-poodle.pdf`
`url: http://www.securityfocus.com/bid/70574`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html`
`url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin`
`↪g-ssl-30.html`
`cert-bund: WID-SEC-2023-0431`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[ return to 192.168.228.209 ]

## 2.6 192.168.228.46

| | |
|---|---|
| Host scan start | Thu Feb 13 09:20:37 2025 UTC |
| Host scan end | Thu Feb 13 12:55:21 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | High |
| 80/tcp | High |
| 443/tcp | Medium |
| 443/tcp | Low |

### 2.6.1 High 443/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          https://192.168.228.46/goform/login
Response(s): Location: https://gbvt1412653528/csfec05640/goform/login
                       This document has moved to a new <a href="https://gbvt14
↪12653528/csfec05640/goform/login">location</a>.
URL:          https://192.168.228.46/config/log_off_page.htm
Response(s): Location: https://gbvt1680250393/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="https://gbvt16
↪80250393/csfec05640/config/log_off_page.htm">location</a>.
URL:          https://192.168.228.46/
Response(s): Location: https://gbvt5205177/csfec05640/
                       This document has moved to a new <a href="https://gbvt52
↪05177/csfec05640/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

. . . continues on next page . . .

... continued from previous page ...

**References**
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20server%20HTTP%20Header%20Injection

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

... continues on next page ...

... continued from previous page ...

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 192.168.228.46 ]

### 2.6.2 High 80/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          http://192.168.228.46/goform/login
Response(s): Location: http://gbvt1690103458/csfec05640/goform/login
                       This document has moved to a new <a href="http://gbvt169
↪0103458/csfec05640/goform/login">location</a>.
URL:          http://192.168.228.46/config/log_off_page.htm
Response(s): Location: http://gbvt167153892/csfec05640/config/log_off_page.htm
```

... continues on next page ...

... continued from previous page ...

```
                        This document has moved to a new <a href="http://gbvt167
↪153892/csfec05640/config/log_off_page.htm">location</a>.
URL:          http://192.168.228.46/
Response(s): Location: http://gbvt566889054/csfec05640/
                        This document has moved to a new <a href="http://gbvt566
↪889054/csfec05640/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**

```
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv
↪er%20HTTP%20Header%20Injection
```

[ return to 192.168.228.46 ]

### 2.6.3 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
```

... continues on next page ...

... continued from previous page ...

↪802067)

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**

cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Product detection result**
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

**Summary**
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

**Vulnerability Detection Method**
Check the used SSL protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_sockets_layer:3.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
`cve: CVE-2016-0800`
`cve: CVE-2014-3566`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://drownattack.com/`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: WID-SEC-2023-0431`
`cert-bund: WID-SEC-2023-0427`
`cert-bund: CB-K18/0094`
`cert-bund: CB-K17/1198`
`cert-bund: CB-K17/1196`
`cert-bund: CB-K16/1828`
`cert-bund: CB-K16/1438`
`cert-bund: CB-K16/1384`
`cert-bund: CB-K16/1141`
`cert-bund: CB-K16/1107`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0792`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0597`
`cert-bund: CB-K16/0459`
`cert-bund: CB-K16/0456`
`cert-bund: CB-K16/0433`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:56C41EB1523E862B33188E1995CD9BA3:OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
↪  (Server certificate)
```

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: `SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048. ↪..`
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: `2021-12-10T12:48:00Z`

**References**
`url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf`

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

... continues on next page ...

... continued from previous page ...

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
The certificate of the remote service expired on 2014-05-02 14:57:19.
Certificate details:
fingerprint (SHA-1)                | 6696D12E5AE3F808071A6F322880541AB2A7DE27
fingerprint (SHA-256)              | 0867B511088F08864EA14C88B426EA3DB5E955D85F5C0B
↪25DFB682BB9B18FA28
issued by                          | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
public key algorithm               | RSA
public key size (bits)             | 1024
serial                             | 56C41EB1523E862B33188E1995CD9BA3
signature algorithm                | md5WithRSAEncryption
subject                            | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
subject alternative names (SAN)    | None
valid from                         | 2013-05-02 14:57:19 UTC
valid until                        | 2014-05-02 14:57:19 UTC
```

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Product detection result**

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

... continues on next page ...

... continued from previous page ...

**Summary**
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

**Impact**
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**

cve: CVE-2015-0204
url: https://freakattack.com
url: http://www.securityfocus.com/bid/71936
url: http://secpod.org/blog/?p=3818
url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac
↪toring-nsa.html
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
. . . continues on next page . . .

... continued from previous page ...

Product: cpe:/a:ietf:secure_sockets_layer:3.0
Method: SSL/TLS: Version Detection
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**

cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
Signature Algorithm:  md5WithRSAEncryption
```

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:

... continues on next page ...

... continued from previous page ...

- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

**References**
`url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/`

[ return to 192.168.228.46 ]

### 2.6.4 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)`

**Summary**
This host is prone to an information disclosure vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

**Impact**
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

**Solution:**
**Solution type:** Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

**Vulnerability Insight**
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

**Vulnerability Detection Method**
Evaluate previous collected information about this service.
Details: `SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ..`
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: `2024-09-30T08:38:05Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2014-3566`
`url: https://www.openssl.org/~bodo/ssl-poodle.pdf`
`url: http://www.securityfocus.com/bid/70574`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html`
`url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin`
`g-ssl-30.html`
`cert-bund: WID-SEC-2023-0431`
`cert-bund: CB-K17/1198`
`cert-bund: CB-K17/1196`
`cert-bund: CB-K16/1828`
`cert-bund: CB-K16/1438`
`cert-bund: CB-K16/1384`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0156`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[ return to 192.168.228.46 ]

## 2.7 192.168.228.98

Host scan start Thu Feb 13 08:51:19 2025 UTC
Host scan end Thu Feb 13 12:22:05 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | High |
| 443/tcp | High |
| 443/tcp | Medium |
| 443/tcp | Low |

### 2.7.1 High 80/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
```

... continues on next page ...

... continued from previous page ...

```
URL:          http://192.168.228.98/goform/login
Response(s): Location: http://gbvt1862644721/csfec05640/goform/login
                       This document has moved to a new <a href="http://gbvt186
↪2644721/csfec05640/goform/login">location</a>.
URL:          http://192.168.228.98/config/log_off_page.htm
Response(s): Location: http://gbvt856395143/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="http://gbvt856
↪395143/csfec05640/config/log_off_page.htm">location</a>.
URL:          http://192.168.228.98/
Response(s): Location: http://gbvt989334981/csfec05640/
                       This document has moved to a new <a href="http://gbvt989
↪334981/csfec05640/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**
`cve: CVE-2019-16645`
`url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv`
`↪er%20HTTP%20Header%20Injection`

[ return to 192.168.228.98 ]

### 2.7.2 High 443/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          https://192.168.228.98/goform/login
Response(s): Location: https://gbvt1235629074/csfec05640/goform/login
                       This document has moved to a new <a href="https://gbvt12
↪35629074/csfec05640/goform/login">location</a>.
URL:          https://192.168.228.98/config/log_off_page.htm
Response(s): Location: https://gbvt954974612/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="https://gbvt95
↪4974612/csfec05640/config/log_off_page.htm">location</a>.
URL:          https://192.168.228.98/
Response(s): Location: https://gbvt1814947150/csfec05640/
                       This document has moved to a new <a href="https://gbvt18
↪14947150/csfec05640/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

. . . continues on next page . . .

... continued from previous page ...

**References**
cve: CVE-2019-16645
url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20server%20HTTP%20Header%20Injection

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

... continues on next page ...

... continued from previous page ...

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 192.168.228.98 ]

### 2.7.3 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Product detection result**
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

**Summary**
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto
↪col and supports one or more ciphers. Those supported ciphers can be found in

... continues on next page ...

... continued from previous page ...

↪the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020
↪67) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

**Vulnerability Detection Method**
Check the used SSL protocols of the services provided by this system.
Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_sockets_layer:3.0
Method: SSL/TLS: Version Detection
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
cve: CVE-2016-0800
cve: CVE-2014-3566
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://drownattack.com/
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-0431
cert-bund: WID-SEC-2023-0427

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K18/0094
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1141
cert-bund: CB-K16/1107
cert-bund: CB-K16/1102
cert-bund: CB-K16/0792
cert-bund: CB-K16/0599
cert-bund: CB-K16/0597
cert-bund: CB-K16/0459
cert-bund: CB-K16/0456
cert-bund: CB-K16/0433
cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

... continues on next page ...

... continued from previous page ...

Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: `SSL/TLS: Report Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
`cve: CVE-2013-2566`
`cve: CVE-2015-2808`
`cve: CVE-2015-4000`
`url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1`
`↪465_update_6.html`
`url: https://bettercrypto.org/`
`url: https://mozilla.github.io/server-side-tls/ssl-config-generator/`
`cert-bund: CB-K21/0067`
`cert-bund: CB-K19/0812`
`cert-bund: CB-K17/1750`
`cert-bund: CB-K16/1593`
`cert-bund: CB-K16/1552`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0617`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0168`
`cert-bund: CB-K16/0121`
`cert-bund: CB-K16/0090`
`cert-bund: CB-K16/0030`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1591`
`cert-bund: CB-K15/1550`
`cert-bund: CB-K15/1517`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:6A91EFCAD910DCBED6601AF44862BB8E:OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
↪  (Server certificate)
```

... continues on next page ...

... continued from previous page ...

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: `SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: `2021-12-10T12:48:00Z`

**References**
`url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf`

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25`
`↪623.1.0.103692)`

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
`The certificate of the remote service expired on 2014-05-02 14:56:42.`
`Certificate details:`

| | |
|---|---|
| fingerprint (SHA-1) | 75ABA59A2211D9B5D0456CC45DAE0E91A85534BC |
| fingerprint (SHA-256) | 46EFD70547D2BB503DC176DD9876091B0512D8966C7D7D4F493825E6D10BE9D2 |
| issued by | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| public key algorithm | RSA |

... continues on next page ...

... continued from previous page ...

| | |
|---|---|
| public key size (bits) | 1024 |
| serial | 6A91EFCAD910DCBED6601AF44862BB8E |
| signature algorithm | md5WithRSAEncryption |
| subject | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| subject alternative names (SAN) | None |
| valid from | 2013-05-02 14:56:42 UTC |
| valid until | 2014-05-02 14:56:42 UTC |

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

**Summary**
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

... continues on next page ...

... continued from previous page ...

'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

**Impact**
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2015-0204
url: https://freakattack.com
url: http://www.securityfocus.com/bid/71936
url: http://secpod.org/blog/?p=3818
url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac
↪toring-nsa.html
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**
`cpe:/a:ietf:secure_sockets_layer:3.0`
`Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)`

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

... continues on next page ...

... continued from previous page ...

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_sockets_layer:3.0
Method: SSL/TLS: Version Detection
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/

... continues on next page ...

... continued from previous page ...

```
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
Signature Algorithm:  md5WithRSAEncryption
```

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1

... continues on next page ...

... continued from previous page ...

or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

**References**
`url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/`

[ return to 192.168.228.98 ]

### 2.7.4 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)`

**Summary**
This host is prone to an information disclosure vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

**Solution:**
**Solution type:** Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

**Vulnerability Detection Method**
Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability .
↪..
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2014-3566
url: https://www.openssl.org/~bodo/ssl-poodle.pdf
url: http://www.securityfocus.com/bid/70574
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin
↪g-ssl-30.html
cert-bund: WID-SEC-2023-0431
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[ return to 192.168.228.98 ]

## 2.8 192.168.228.99

Host scan start Thu Feb 13 08:51:44 2025 UTC
Host scan end Thu Feb 13 12:23:31 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | High |
| 80/tcp | High |
| 443/tcp | Medium |
| 443/tcp | Low |

### 2.8.1 High 443/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          https://192.168.228.99/goform/login
Response(s): Location: https://gbvt253427644/csfec05640/goform/login
                       This document has moved to a new <a href="https://gbvt25
↪3427644/csfec05640/goform/login">location</a>.
URL:          https://192.168.228.99/config/log_off_page.htm
Response(s): Location: https://gbvt1733899510/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="https://gbvt17
↪33899510/csfec05640/config/log_off_page.htm">location</a>.
URL:          https://192.168.228.99/
Response(s): Location: https://gbvt1623855624/csfec05640/
                       This document has moved to a new <a href="https://gbvt16
↪23855624/csfec05640/">location</a>.
```

... continues on next page ...

... continued from previous page ...

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**
For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**
`cve: CVE-2019-16645`
`url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20serv`
`↪er%20HTTP%20Header%20Injection`

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.`
`↪802067)`

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

... continues on next page ...

... continued from previous page ...

'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 192.168.228.99 ]

### 2.8.2 High 80/tcp

High (CVSS: 8.6)
NVT: Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check

**Summary**
Embedthis GoAhead is prone to an HTTP header injection vulnerability.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
It was possible to inject a host header and create a manipulated link via a HTTP
↪ POST-request to:
URL:          http://192.168.228.99/goform/login
Response(s): Location: http://gbvt1712793079/csfec05640/goform/login
                       This document has moved to a new <a href="http://gbvt171
↪2793079/csfec05640/goform/login">location</a>.
URL:          http://192.168.228.99/config/log_off_page.htm
Response(s): Location: http://gbvt1390997836/csfec05640/config/log_off_page.htm
                       This document has moved to a new <a href="http://gbvt139
↪0997836/csfec05640/config/log_off_page.htm">location</a>.
URL:          http://192.168.228.99/
Response(s): Location: http://gbvt335811440/csfec05640/
                       This document has moved to a new <a href="http://gbvt335
↪811440/csfec05640/">location</a>.
```

**Impact**
An attacker can potentially use this vulnerability in a phishing attack.

**Solution:**
**Solution type:** WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

**Affected Software/OS**
Embedthis GoAhead version 2.5.0 is known to be affected. Other versions might be affected as well.

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

For certain pages, Embedthis GoAhead creates links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker.

**Vulnerability Detection Method**
Send multiple crafted HTTP POST requests and checks the responses.
Details: `Embedthis GoAhead 2.5.0 HTTP Header Injection Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.114133
Version used: `2024-09-25T05:06:11Z`

**References**
`cve: CVE-2019-16645`
`url: https://github.com/Ramikan/Vulnerabilities/blob/master/GoAhead%20Web%20server%20HTTP%20Header%20Injection`

[ return to 192.168.228.99 ]

### 2.8.3 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)`

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
```
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
```

... continues on next page ...

... continued from previous page ...

TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Product detection result**
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

... continues on next page ...

... continued from previous page ...

**Summary**
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
`In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto`
`↪col and supports one or more ciphers. Those supported ciphers can be found in`
`↪the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020`
`↪67) VT.`

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

**Vulnerability Detection Method**
Check the used SSL protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_sockets_layer:3.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2016-0800
cve: CVE-2014-3566
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://drownattack.com/
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-0431
cert-bund: WID-SEC-2023-0427
cert-bund: CB-K18/0094
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1141
cert-bund: CB-K16/1107
cert-bund: CB-K16/1102
cert-bund: CB-K16/0792
cert-bund: CB-K16/0599
cert-bund: CB-K16/0597
cert-bund: CB-K16/0459
cert-bund: CB-K16/0456
cert-bund: CB-K16/0433
cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:547FE9AB403D8A6925D21D2612AB4EFB:OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
↪  (Server certificate)
```

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**

... continues on next page ...

... continued from previous page ...

SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

**References**
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
The certificate of the remote service expired on 2014-05-02 14:56:35.
Certificate details:

| | |
|---|---|
| fingerprint (SHA-1) | 23BDA14D867573D478845078867FAA01134CD487 |
| fingerprint (SHA-256) | 07EEC63A1638B86465927BAD5BF0A8A546C710A30B6559 ↪7A4DF21192562D21D0 |
| issued by | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| public key algorithm | RSA |
| public key size (bits) | 1024 |
| serial | 547FE9AB403D8A6925D21D2612AB4EFB |
| signature algorithm | md5WithRSAEncryption |
| subject | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \ |
| subject alternative names (SAN) | None |
| valid from | 2013-05-02 14:56:35 UTC |
| valid until | 2014-05-02 14:56:35 UTC |

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**
`cpe:/a:ietf:secure_sockets_layer:3.0`
`Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)`

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
```
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-09-27T05:05:23Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_sockets_layer:3.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Product detection result**

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

... continues on next page ...

... continued from previous page ...

**Summary**
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

**Impact**
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**

cve: CVE-2015-0204
url: https://freakattack.com
url: http://www.securityfocus.com/bid/71936
url: http://secpod.org/blog/?p=3818
url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac
↪toring-nsa.html
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

**Summary**
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
Signature Algorithm:  md5WithRSAEncryption
```

**Solution:**
**Solution type:** Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

**Vulnerability Detection Method**
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

**References**
```
url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-
↪sha-1-based-signature-algorithms/
```

[ return to 192.168.228.99 ]

### 2.8.4 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)

**Summary**
This host is prone to an information disclosure vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

**Solution:**
**Solution type:** Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

**Vulnerability Insight**
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

**Vulnerability Detection Method**
Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ...
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: 2024-09-30T08:38:05Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security

... continues on next page ...

... continued from previous page ...

Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

**References**

cve: CVE-2014-3566
url: https://www.openssl.org/~bodo/ssl-poodle.pdf
url: http://www.securityfocus.com/bid/70574
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin
↪g-ssl-30.html
cert-bund: WID-SEC-2023-0431
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[ return to 192.168.228.99 ]

## 2.9 192.168.228.101

Host scan start Thu Feb 13 12:35:13 2025 UTC
Host scan end

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | High |
| 443/tcp | Medium |
| 443/tcp | Low |

### 2.9.1 High 443/tcp

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

**Summary**
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
```
'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
```

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Affected Software/OS**
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

**Vulnerability Detection Method**
Details: `SSL/TLS: Report Vulnerable Cipher Suites for HTTPS`
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: `2024-09-30T08:38:05Z`

**References**
```
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
```

. . . continues on next page . . .

... continued from previous page ...

```
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[ return to 192.168.228.101 ]

### 2.9.2 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Summary**
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto
↪col and supports one or more ciphers. Those supported ciphers can be found in
↪the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020
↪67) VT.
```

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

**Vulnerability Detection Method**
Check the used SSL protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: `2024-09-27T05:05:23Z`

**References**
`cve: CVE-2016-0800`
`cve: CVE-2014-3566`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://drownattack.com/`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters`
`↪-report-2014`
`cert-bund: WID-SEC-2023-0431`
`cert-bund: WID-SEC-2023-0427`
`cert-bund: CB-K18/0094`
`cert-bund: CB-K17/1198`
`cert-bund: CB-K17/1196`
`cert-bund: CB-K16/1828`
`cert-bund: CB-K16/1438`
`cert-bund: CB-K16/1384`
`cert-bund: CB-K16/1141`
`cert-bund: CB-K16/1107`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0792`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0597`
`cert-bund: CB-K16/0459`
`cert-bund: CB-K16/0456`
`cert-bund: CB-K16/0433`
`cert-bund: CB-K16/0424`
`cert-bund: CB-K16/0415`
`cert-bund: CB-K16/0413`
`cert-bund: CB-K16/0374`
`cert-bund: CB-K16/0367`
`cert-bund: CB-K16/0331`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

**Summary**
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

... continues on next page ...

... continued from previous page ...

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
```

**Solution:**
**Solution type:** Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

**Vulnerability Insight**
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

**Vulnerability Detection Method**
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2024-09-27T05:05:23Z

**References**

```
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
The certificate of the remote service expired on 2014-05-02 14:54:44.
Certificate details:
fingerprint (SHA-1)              | 9339DFF83A624ECE9053059F15A54E021C2992FB
fingerprint (SHA-256)            | C191C076B03A16B15024BB0432589157E99DC36F6C31B3
↪7A80AAC02422716553
issued by                        | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
public key algorithm             | RSA
public key size (bits)           | 1024
serial                           | 7AE6FA572338B56EA5D6E305550583D4
signature algorithm              | md5WithRSAEncryption
subject                          | OU=\ ,O=\ ,CN=0.0.0.0,L=\ ,ST=\ ,C=\ \
subject alternative names (SAN)  | None
valid from                       | 2013-05-02 14:54:44 UTC
valid until                      | 2014-05-02 14:54:44 UTC
```

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `2024-06-14T05:05:48Z`

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Summary**
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

... continues on next page ...

... continued from previous page ...

'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

**Impact**
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

**Solution:**
**Solution type:** VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

**Affected Software/OS**
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

**Vulnerability Insight**
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

**Vulnerability Detection Method**
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: 2024-09-30T08:38:05Z

**References**
cve: CVE-2015-0204
url: https://freakattack.com
url: http://www.securityfocus.com/bid/71936
url: http://secpod.org/blog/?p=3818
url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac
↪toring-nsa.html
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**

```
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

**Impact**

... continues on next page ...

... continued from previous page ...

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-09-27T05:05:23Z`

**References**
`cve: CVE-2011-3389`
`cve: CVE-2015-0204`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://datatracker.ietf.org/doc/rfc8996/`
`url: https://vnhacker.blogspot.com/2011/09/beast.html`
`url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1266`
`cert-bund: CB-K15/0850`
`cert-bund: CB-K15/0764`
`cert-bund: CB-K15/0720`
`cert-bund: CB-K15/0548`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

[ return to 192.168.228.101 ]

### 2.9.3 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

**Summary**
This host is prone to an information disclosure vulnerability.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

**Solution:**
**Solution type:** Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

**Vulnerability Insight**
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

**Vulnerability Detection Method**
Evaluate previous collected information about this service.
Details: `SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ..`
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: `2024-09-30T08:38:05Z`

**References**
`cve: CVE-2014-3566`
`url: https://www.openssl.org/~bodo/ssl-poodle.pdf`
`url: http://www.securityfocus.com/bid/70574`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html`
`url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin g-ssl-30.html`
`cert-bund: WID-SEC-2023-0431`
`cert-bund: CB-K17/1198`
`cert-bund: CB-K17/1196`
`cert-bund: CB-K16/1828`
`cert-bund: CB-K16/1438`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[ return to 192.168.228.101 ]

## 2.10 192.168.228.151

| | |
|---|---|
| Host scan start | Thu Feb 13 08:01:52 2025 UTC |
| Host scan end | Thu Feb 13 08:21:26 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 135/tcp | Medium |

### 2.10.1 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

**Summary**
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

**Quality of Detection (QoD):** 80%

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Result**

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49664]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49664]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49664]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.228.151[49664]
     Annotation: KeyIso
Port: 49665/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49665]
Port: 49666/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49666]
     Annotation: Windows Event Log
Port: 49667/tcp
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49667]
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49667]
Port: 49669/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49669]
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49669]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49669]
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49669]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.151[49669]
Port: 49671/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.228.151[49671]
```

... continues on next page ...

... continued from previous page ...

```
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

**Impact**
An attacker may use this fact to gain more knowledge about the remote host.

**Solution:**
**Solution type:** Mitigation
Filter incoming traffic to this ports.

**Vulnerability Detection Method**
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: 2022-06-03T10:17:07Z

[ return to 192.168.228.151 ]

## 2.11 192.168.228.120

| | |
|---|---|
| Host scan start | Thu Feb 13 08:01:52 2025 UTC |
| Host scan end | Thu Feb 13 08:21:28 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 135/tcp | Medium |

### 2.11.1 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

**Summary**
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.228.120[49664]
```

... continues on next page ...

... continued from previous page ...

```
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
      UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49664]
      Annotation: Ngc Pop Key Service
      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49664]
      Annotation: Ngc Pop Key Service
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:192.168.228.120[49664]
      Annotation: KeyIso
Port: 49665/tcp
      UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49665]
Port: 49666/tcp
      UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49666]
      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49666]
Port: 49667/tcp
      UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49667]
      Annotation: Windows Event Log
Port: 49669/tcp
      UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49669]
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49669]
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49669]
      UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49669]
      UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
      Endpoint: ncacn_ip_tcp:192.168.228.120[49669]
Port: 49683/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:192.168.228.120[49683]
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

**Impact**

An attacker may use this fact to gain more knowledge about the remote host.

... continues on next page ...

... continued from previous page ...

**Solution:**
**Solution type:** Mitigation
Filter incoming traffic to this ports.

**Vulnerability Detection Method**
Details: `DCE/RPC and MSRPC Services Enumeration Reporting`
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: `2022-06-03T10:17:07Z`

[ return to 192.168.228.120 ]

# Scan Report

February 15, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Réseaux_Users_ESA_UL". The scan started at Sat Feb 15 09:51:56 2025 UTC and ended at . The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 192.168.224.161 | 0 | 2 | 0 | 0 | 0 |
| 192.168.224.132 | 0 | 2 | 1 | 0 | 0 |
| Total: 2 | 0 | 4 | 1 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 5 results selected by the filtering described above. Before filtering there were 39 results.

# 2 Results per Host

## 2.1 192.168.224.161

| | |
|---|---|
| Host scan start | Sat Feb 15 09:52:52 2025 UTC |
| Host scan end | Sat Feb 15 10:03:50 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 22/tcp | Medium |

### 2.1.1 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Host Key Algorithm(s) (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565`
`↪)`

**Summary**

. . . continues on next page . . .

... continued from previous page ...

The remote SSH server is configured to allow / support weak host key algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
-------------------------------------------------------------------------------
↪---------
ssh-dss            | Digital Signature Algorithm (DSA) / Digital Signature Stand
↪ard (DSS)
```

**Solution:**
**Solution type:** Mitigation
Disable the reported weak host key algorithm(s).

**Vulnerability Detection Method**
Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: `Weak Host Key Algorithm(s) (SSH)`
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc8332`
`url: https://www.rfc-editor.org/rfc/rfc8709`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6`

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Product detection result**

```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

**Summary**

... continues on next page ...

... continued from previous page ...

The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm               | Reason
-------------------------------------------------------------------------------
↪---
diffie-hellman-group1-sha1 | Using Oakley Group 2 (a 1024-bit MODP group) and SH
↪A-1
```

**Impact**

An attacker can quickly break individual connections.

**Solution:**

**Solution type:** Mitigation

Disable the reported weak KEX algorithm(s)

- 1024-bit MODP group / prime KEX algorithms:

Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

**Vulnerability Insight**

- 1024-bit MODP group / prime KEX algorithms:

Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

**Vulnerability Detection Method**

Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:

- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key

Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**

Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**

... continues on next page ...

... continued from previous page ...

```
url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5
```

[ return to 192.168.224.161 ]

## 2.2 192.168.224.132

Host scan start Sat Feb 15 09:52:52 2025 UTC
Host scan end Sat Feb 15 10:02:19 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 22/tcp | Medium |
| 22/tcp | Low |

### 2.2.1 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Host Key Algorithm(s) (SSH)

**Product detection result**

```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

**Summary**
The remote SSH server is configured to allow / support weak host key algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
-------------------------------------------------------------------------------
↪---------
ssh-dss            | Digital Signature Algorithm (DSA) / Digital Signature Stand
↪ard (DSS)
```

**Solution:**
**Solution type:** Mitigation
Disable the reported weak host key algorithm(s).

... continues on next page ...

... continued from previous page ...

**Vulnerability Detection Method**
Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: `Weak Host Key Algorithm(s) (SSH)`
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc8332`
`url: https://www.rfc-editor.org/rfc/rfc8709`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6`

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565`
`↪)`

**Summary**
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                | Reason
-----------------------------------------------------------------------------
↪---
diffie-hellman-group1-sha1 | Using Oakley Group 2 (a 1024-bit MODP group) and SH
↪A-1
```

**Impact**
An attacker can quickly break individual connections.

**Solution:**
**Solution type:** Mitigation

... continues on next page ...

... continued from previous page ...

Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

**Vulnerability Insight**
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

**Vulnerability Detection Method**
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://weakdh.org/sysadmin.html`
`url: https://www.rfc-editor.org/rfc/rfc9142`
`url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem`
`url: https://www.rfc-editor.org/rfc/rfc6194`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5`

[ return to 192.168.224.132 ]

### 2.2.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565`

... continues on next page ...

... continued from previous page ...

↪)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s):`
`hmac-md5`
`The remote SSH server supports the following weak server-to-client MAC algorithm ↪(s):`
`hmac-md5`

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[ return to 192.168.224.132 ]

# Scan Report

February 13, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Public_IP_Adress_UL". The scan started at Wed Feb 12 13:27:29 2025 UTC and ended at Wed Feb 12 18:01:59 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 41.207.188.28 | 0 | 2 | 0 | 0 | 0 |
| 41.207.188.29 | 0 | 2 | 0 | 0 | 0 |
| Total: 2 | 0 | 4 | 0 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 4 results selected by the filtering described above. Before filtering there were 57 results.

# 2 Results per Host

## 2.1 41.207.188.28

| | |
|---|---|
| Host scan start | Wed Feb 12 13:29:03 2025 UTC |
| Host scan end | Wed Feb 12 17:53:46 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | Medium |
| 80/tcp | Medium |

### 2.1.1 Medium 443/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25`
`↪623.1.0.103692)`

. . . continues on next page . . .

... continued from previous page ...

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**

```
The certificate of the remote service expired on 2021-07-17 07:30:14.
Certificate details:
fingerprint (SHA-1)              | E5037E811D542E28B10BDE76575E4F6E4CA2CCCA
fingerprint (SHA-256)            | 42C97AFB101233F2F01C5369D778293316442221E81820
↪AF7E17AB1F3F333511
issued by                        | CN=Go Daddy Secure Certificate Authority - G2,
↪OU=http://certs.godaddy.com/repository/,O=GoDaddy.com\, Inc.,L=Scottsdale,ST=A
↪rizona,C=US
public key algorithm             | RSA
public key size (bits)           | 2048
serial                           | 00E4FEA1131DA14AEB
signature algorithm              | sha256WithRSAEncryption
subject                          | CN=captive-portal.peplink.com,OU=Domain Contro
↪l Validated
subject alternative names (SAN)  | captive-portal.peplink.com, www.captive-portal
↪.peplink.com
valid from                       | 2019-07-17 07:30:14 UTC
valid until                      | 2021-07-17 07:30:14 UTC
```

**Solution:**
**Solution type:** Mitigation
Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

[ return to 41.207.188.28 ]

### 2.1.2 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The following input fields were identified (URL:input name):`
`http://41.207.188.28/cgi-bin/MANGA/index.cgi:password`

**Impact**
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

**References**
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[ return to 41.207.188.28 ]

## 2.2 41.207.188.29

| | |
|---|---|
| Host scan start | Wed Feb 12 13:29:03 2025 UTC |
| Host scan end | Wed Feb 12 18:01:56 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 443/tcp | Medium |
| 80/tcp | Medium |

### 2.2.1 Medium 443/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

**Product detection result**
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
The certificate of the remote service expired on 2021-07-17 07:30:14.
Certificate details:

| | |
|---|---|
| fingerprint (SHA-1) | E5037E811D542E28B10BDE76575E4F6E4CA2CCCA |
| fingerprint (SHA-256) | 42C97AFB101233F2F01C5369D778293316442221E81820 ↪AF7E17AB1F3F333511 |
| issued by | CN=Go Daddy Secure Certificate Authority - G2, ↪OU=http://certs.godaddy.com/repository/,O=GoDaddy.com\, Inc.,L=Scottsdale,ST=A ↪rizona,C=US |
| public key algorithm | RSA |
| public key size (bits) | 2048 |
| serial | 00E4FEA1131DA14AEB |
| signature algorithm | sha256WithRSAEncryption |
| subject | CN=captive-portal.peplink.com,OU=Domain Contro ↪l Validated |
| subject alternative names (SAN) | captive-portal.peplink.com, www.captive-portal ↪.peplink.com |
| valid from | 2019-07-17 07:30:14 UTC |
| valid until | 2021-07-17 07:30:14 UTC |

**Solution:**
**Solution type:** Mitigation

. . . continues on next page . . .

... continued from previous page ...

Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

[ return to 41.207.188.29 ]

### 2.2.2 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The following input fields were identified (URL:input name):
http://41.207.188.29/cgi-bin/MANGA/index.cgi:password
```

**Impact**
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

... continues on next page ...

... continued from previous page ...

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

**References**
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[ return to 41.207.188.29 ]

# Scan Report

February 12, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Portail academique (étudiants)". The scan started at Wed Feb 12 10:40:28 2025 UTC and ended at Wed Feb 12 13:18:11 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 172.20.1.3 etu.univ-lome.tg | 0 | 3 | 0 | 0 | 0 |
| Total: 1 | 0 | 3 | 0 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 3 results selected by the filtering described above. Before filtering there were 88 results.

# 2 Results per Host

## 2.1 172.20.1.3

| | |
|---|---|
| Host scan start | Wed Feb 12 10:41:17 2025 UTC |
| Host scan end | Wed Feb 12 13:18:05 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 22/tcp | Medium |
| 443/tcp | Medium |

### 2.1.1 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↪)`

... continues on next page ...

... continued from previous page ...

**Summary**
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                     | Reason
-------------------------------------------
diffie-hellman-group-exchange-sha1 | Using SHA-1
```

**Impact**
An attacker can quickly break individual connections.

**Solution:**
**Solution type:** Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

**Vulnerability Insight**
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

**Vulnerability Detection Method**
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://weakdh.org/sysadmin.html`

... continues on next page ...

... continued from previous page ...

url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak encryption algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
aes128-cbc
aes256-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
aes128-cbc
aes256-cbc

**Solution:**
**Solution type:** Mitigation
Disable the reported weak encryption algorithm(s).

**Vulnerability Insight**
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

**Vulnerability Detection Method**
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:

... continues on next page ...

... continued from previous page ...

- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms

Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc8758`
`url: https://www.kb.cert.org/vuls/id/958563`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3`

[ return to 172.20.1.3 ]

### 2.1.2 Medium 443/tcp

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

**Summary**
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

**Quality of Detection (QoD):** 99%

**Vulnerability Detection Result**
`The web server has the following HTTP methods enabled: TRACE`

**Impact**
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

**Solution:**
**Solution type:** Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

**Affected Software/OS**
Web servers with enabled TRACE and/or TRACK methods.

... continues on next page ...

... continued from previous page ...

**Vulnerability Insight**
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

**Vulnerability Detection Method**
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2023-08-01T13:29:10Z`

**References**
`cve: CVE-2003-1567`
`cve: CVE-2004-2320`
`cve: CVE-2004-2763`
`cve: CVE-2005-3398`
`cve: CVE-2006-4683`
`cve: CVE-2007-3008`
`cve: CVE-2008-7253`
`cve: CVE-2009-2823`
`cve: CVE-2010-0386`
`cve: CVE-2012-2223`
`cve: CVE-2014-7883`
`url: http://www.kb.cert.org/vuls/id/288308`
`url: http://www.securityfocus.com/bid/11604`
`url: http://www.securityfocus.com/bid/15222`
`url: http://www.securityfocus.com/bid/19915`
`url: http://www.securityfocus.com/bid/24456`
`url: http://www.securityfocus.com/bid/33374`
`url: http://www.securityfocus.com/bid/36956`
`url: http://www.securityfocus.com/bid/36990`
`url: http://www.securityfocus.com/bid/37995`
`url: http://www.securityfocus.com/bid/9506`
`url: http://www.securityfocus.com/bid/9561`
`url: http://www.kb.cert.org/vuls/id/867593`
`url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable`
`url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac`
`↪e-verbs/ba-p/784482`
`url: https://owasp.org/www-community/attacks/Cross_Site_Tracing`
`cert-bund: CB-K14/0981`
`dfn-cert: DFN-CERT-2021-1825`
`dfn-cert: DFN-CERT-2014-1018`
`dfn-cert: DFN-CERT-2010-0020`

[ return to 172.20.1.3 ]

This file was automatically generated.

# Scan Report

February 12, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Site d'apprentissage en ligne". The scan started at Wed Feb 12 10:41:38 2025 UTC and ended at Wed Feb 12 11:36:40 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 172.20.1.6 elearn.univ-lome.tg | 0 | 2 | 1 | 0 | 0 |
| Total: 1 | 0 | 2 | 1 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 3 results selected by the filtering described above. Before filtering there were 97 results.

# 2 Results per Host

## 2.1 172.20.1.6

| | |
|---|---|
| Host scan start | Wed Feb 12 10:42:34 2025 UTC |
| Host scan end | Wed Feb 12 11:36:35 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 8181/tcp | Medium |
| 22/tcp | Low |

### 2.1.1 Medium 8181/tcp

Medium (CVSS: 5.0)
NVT: Missing 'HttpOnly' Cookie Attribute (HTTP)

**Summary**
The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP cookie.

**Quality of Detection (QoD):** 70%

. . . continues on next page . . .

... continued from previous page ...

**Vulnerability Detection Result**

```
The cookie(s):
Set-Cookie: MoodleSession=***replaced***; path=/; secure
is/are missing the "HttpOnly" cookie attribute.
```

**Solution:**
**Solution type:** Mitigation
- Set the 'HttpOnly' cookie attribute for any session cookie
- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

**Affected Software/OS**
Any web application with session handling in cookies.

**Vulnerability Insight**
The flaw exists if a session cookie is not using the 'HttpOnly' cookie attribute.
This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

**Vulnerability Detection Method**
Checks all cookies sent by the remote HTTP web server / application for a missing 'HttpOnly' cookie attribute.
Details: `Missing 'HttpOnly' Cookie Attribute (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.105925
Version used: `2024-01-12T16:12:12Z`

**References**

```
url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6
url: https://owasp.org/www-community/HttpOnly
url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0
↪02)
```

Medium (CVSS: 5.0)
NVT: Source Control Management (SCM) Files/Folders Accessible (HTTP)

**Summary**
The script attempts to identify files/folders of a SCM accessible at the webserver.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**

```
The following SCM files/folders were identified:
Match:      0000000000000000000000000000000000000000 c6e727732a7f3f1060b1c1fbd78
↪75746db5f1000 root <root@moniteur.univ-lome.tg> 1695925148 +0000
clone: from g
↪it://git.moodle.org/moodle.git
```

... continues on next page ...

... continued from previous page ...

```
c6e727732a7f3f1060b1c1fbd7875746db5f1000 da9ebc40f66f3a4a44c3f888a0d8318ee86e172
↪a root <root@moniteur.univ-lome.tg> 1695925233 +0000 checkout: moving from mas
↪ter to MOODLE_402_STABLE
Used regex: ^[a-f0-9]{40} [a-f0-9]{40}
URL:        https://elearn.univ-lome.tg:8181/.git/logs/HEAD
Match:      [core]
[remote "origin"]
[branch "master"]
[branch "MOODLE_402_STABLE"]
Used regex: ^\[(core|receive|(remote|branch) .+)\]$
URL:        https://elearn.univ-lome.tg:8181/.git/config
Match:      # git ls-files --others --exclude-from=.git/info/exclude
Used regex: ^# git ls-files
URL:        https://elearn.univ-lome.tg:8181/.git/info/exclude
Match:      DIRC
Used regex: ^DIRC
URL:        https://elearn.univ-lome.tg:8181/.git/index
Match:      Unnamed repository; edit this file 'description' to name the reposit
↪ory.
Used regex: ^Unnamed repository
URL:        https://elearn.univ-lome.tg:8181/.git/description
Match:      ref: refs/heads/MOODLE_402_STABLE
Used regex: ^ref: refs/
URL:        https://elearn.univ-lome.tg:8181/.git/HEAD
```

**Impact**
Based on the information provided in these files/folders an attacker might be able to gather additional info about the structure of the system and its applications.

**Solution:**
**Solution type:** Mitigation
Restrict access to the SCM files/folders for authorized systems only.

**Vulnerability Insight**
Currently the script is checking for files/folders of the following SCM software:
- Git (.git)
- Mercurial (.hg)
- Bazaar (.bzr)
- CVS (CVS/Root, CVS/Entries)
- Subversion (.svn)

**Vulnerability Detection Method**
Check the response if SCM files/folders are accessible.
Details: `Source Control Management (SCM) Files/Folders Accessible (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.111084
Version used: `2023-08-01T13:29:10Z`

... continues on next page ...

... continued from previous page ...

**References**
url: http://pen-testing.sans.org/blog/pen-testing/2012/12/06/all-your-svn-are-be
↪long-to-us
url: https://github.com/anantshri/svn-extractor
url: https://blog.skullsecurity.org/2012/using-git-clone-to-get-pwn3d
url: https://blog.netspi.com/dumping-git-data-from-misconfigured-web-servers/
url: http://resources.infosecinstitute.com/hacking-svn-git-and-mercurial/

[ return to 172.20.1.6 ]

### 2.1.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:

... continues on next page ...

... continued from previous page ...

- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm

Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[ return to 172.20.1.6 ]

# Scan Report

February 13, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Switchs_UL". The scan started at Thu Feb 13 07:21:00 2025 UTC and ended at Thu Feb 13 07:45:50 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 192.168.254.2 | 0 | 2 | 1 | 0 | 0 |
| Total: 1 | 0 | 2 | 1 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 3 results selected by the filtering described above. Before filtering there were 17 results.

# 2 Results per Host

## 2.1 192.168.254.2

| | |
|---|---|
| Host scan start | Thu Feb 13 07:21:54 2025 UTC |
| Host scan end | Thu Feb 13 07:45:45 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 22/tcp | Medium |
| 23/tcp | Medium |
| 22/tcp | Low |

### 2.1.1 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↪)`

... continues on next page ...

... continued from previous page ...

**Summary**
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                     | Reason
-------------------------------------------
diffie-hellman-group-exchange-sha1 | Using SHA-1
```

**Impact**
An attacker can quickly break individual connections.

**Solution:**
**Solution type:** Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

**Vulnerability Insight**
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

**Vulnerability Detection Method**
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2024-06-14T05:05:48Z`

**Product Detection Result**
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
`url: https://weakdh.org/sysadmin.html`

... continues on next page ...

... continued from previous page ...

```
url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5
```

[ return to 192.168.254.2 ]

### 2.1.2 Medium 23/tcp

Medium (CVSS: 4.8)
NVT: Telnet Unencrypted Cleartext Login

**Summary**
The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.

**Solution:**
**Solution type:** Mitigation
Replace Telnet with a protocol like SSH which supports encrypted connections.

**Vulnerability Detection Method**
Details: `Telnet Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108522
Version used: `2023-10-13T05:06:09Z`

[ return to 192.168.254.2 ]

### 2.1.3 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

**Product detection result**
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565`

... continues on next page ...

... continued from previous page ...

↪)

**Summary**
The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s):
hmac-sha1-96
The remote SSH server supports the following weak server-to-client MAC algorithm ↪(s):
hmac-sha1-96

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**Product Detection Result**
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

**References**
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[ return to 192.168.254.2 ]

# Scan Report

February 13, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Réseaux_Users_FDS_UL". The scan started at Thu Feb 13 07:25:11 2025 UTC and ended at Thu Feb 13 08:18:13 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 192.168.216.47 | 0 | 2 | 0 | 0 | 0 |
| Total: 1 | 0 | 2 | 0 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 2 results selected by the filtering described above. Before filtering there were 37 results.

# 2 Results per Host

## 2.1 192.168.216.47

| | |
|---|---|
| Host scan start | Thu Feb 13 07:26:27 2025 UTC |
| Host scan end | Thu Feb 13 08:18:10 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | Medium |

### 2.1.1 Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Missing 'HttpOnly' Cookie Attribute (HTTP)

**Summary**
The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP cookie.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
`The cookie(s):`

. . . continues on next page . . .

... continued from previous page ...

```
Set-Cookie: COOKIE=ac14013907cec701; PATH=/; MAXAGE=***replaced***; VERSION=1
is/are missing the "HttpOnly" cookie attribute.
```

**Solution:**
**Solution type:** Mitigation
- Set the 'HttpOnly' cookie attribute for any session cookie
- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

**Affected Software/OS**
Any web application with session handling in cookies.

**Vulnerability Insight**
The flaw exists if a session cookie is not using the 'HttpOnly' cookie attribute.
This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

**Vulnerability Detection Method**
Checks all cookies sent by the remote HTTP web server / application for a missing 'HttpOnly' cookie attribute.
Details: `Missing 'HttpOnly' Cookie Attribute (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.105925
Version used: `2024-01-12T16:12:12Z`

**References**
`url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6`
`url: https://owasp.org/www-community/HttpOnly`
`url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0`
`↪02)`

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The following input fields were identified (URL:input name):
http://192.168.216.47/:password
```

**Impact**

... continues on next page ...

... continued from previous page ...

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

**References**
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[ return to 192.168.216.47 ]

# Scan Report

February 14, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Réseaux_Users_EPL_UL". The scan started at Thu Feb 13 08:30:26 2025 UTC and ended at Fri Feb 14 01:39:11 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 192.168.223.150 | 0 | 1 | 0 | 0 | 0 |
| Total: 1 | 0 | 1 | 0 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains result 1 of the 1 results selected by the filtering above. Before filtering there were 183 results.

# 2 Results per Host

## 2.1 192.168.223.150

| | |
|---|---|
| Host scan start | Thu Feb 13 09:05:56 2025 UTC |
| Host scan end | Fri Feb 14 01:39:03 2025 UTC |

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | Medium |

### 2.1.1 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`The following URLs requires Basic Authentication (URL:realm name):`

... continues on next page ...

... continued from previous page ...

```
http://192.168.223.150/:"TP-LINK Wireless N Access Point WA801N"
http://192.168.223.150/dynaform/css_help.css:"TP-LINK Wireless N Access Point WA
↪801N"
http://192.168.223.150/dynaform/css_main.css:"TP-LINK Wireless N Access Point WA
↪801N"
```

**Impact**
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

**Solution:**
**Solution type:** Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

**Affected Software/OS**
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

**Vulnerability Detection Method**
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

**References**
```
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html
```

[ return to 192.168.223.150 ]