

# Scan Report

March 3, 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 “HVENO-NETWORK-SCAN”. The scan started at Mon Mar 3 15:58:10 2025 UTC and ended at Mon Mar 3 18:02:38 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

<b>1</b>	<b>Result Overview</b>	<b>2</b>
<b>2</b>	<b>Results per Host</b>	<b>3</b>
2.1	192.168.68.110 . . . . .	3
2.1.1	High 4595/tcp . . . . .	3
2.1.2	High 4596/tcp . . . . .	7
2.1.3	Medium 3389/tcp . . . . .	10
2.1.4	Medium 135/tcp . . . . .	14
2.1.5	Medium 4595/tcp . . . . .	16
2.1.6	Medium 4596/tcp . . . . .	19
2.1.7	Low general/icmp . . . . .	23
2.2	192.168.71.247 . . . . .	24
2.2.1	Medium 443/tcp . . . . .	24
2.2.2	Low general/tcp . . . . .	29
2.2.3	Low general/icmp . . . . .	31
2.3	192.168.71.250 . . . . .	32
2.3.1	Medium 443/tcp . . . . .	32
2.3.2	Low general/icmp . . . . .	34
2.3.3	Low general/tcp . . . . .	35
2.4	192.168.71.246 . . . . .	36
2.4.1	Medium 443/tcp . . . . .	36
2.4.2	Low general/tcp . . . . .	38

2.4.3	Low general/icmp	39
2.5	192.168.68.1	40
2.5.1	Medium 443/tcp	40
2.5.2	Low general/tcp	42
2.5.3	Low general/icmp	43
2.6	192.168.71.248	44
2.6.1	Medium 443/tcp	44
2.6.2	Low general/icmp	46
2.6.3	Low general/tcp	47
2.7	192.168.71.249	48
2.7.1	Medium 443/tcp	48
2.7.2	Low general/icmp	50
2.7.3	Low general/tcp	51
2.8	192.168.68.106	52
2.8.1	Medium 135/tcp	52
2.9	192.168.68.83	54
2.9.1	Medium 443/tcp	55
2.10	192.168.68.87	58
2.10.1	Medium 9000/tcp	58
2.10.2	Medium 10101/tcp	62
2.10.3	Medium 8009/tcp	66
2.10.4	Medium 8443/tcp	69
2.10.5	Medium 10001/tcp	73
2.10.6	Low general/icmp	77
2.10.7	Low general/tcp	78
2.11	192.168.68.90	79
2.11.1	Medium 10101/tcp	79
2.11.2	Medium 8443/tcp	83
2.11.3	Medium 8009/tcp	87
2.11.4	Medium 10001/tcp	90
2.11.5	Medium 9000/tcp	94
2.11.6	Low general/tcp	98
2.11.7	Low general/icmp	99
2.12	192.168.68.56	100
2.12.1	Medium 9000/tcp	100
2.12.2	Medium 10101/tcp	104
2.12.3	Medium 8443/tcp	108
2.12.4	Medium 10001/tcp	111
2.12.5	Medium 8009/tcp	115
2.12.6	Low general/icmp	119

2.12.7	Low general/tcp	120
2.13	192.168.68.58	121
2.13.1	Medium 8443/tcp	121
2.13.2	Medium 9000/tcp	123
2.13.3	Medium 10001/tcp	124
2.13.4	Low general/tcp	125
2.13.5	Low general/icmp	126
2.14	192.168.68.86	127
2.14.1	Low general/icmp	127
2.14.2	Low general/tcp	129
2.15	192.168.68.88	130
2.15.1	Low general/tcp	130
2.15.2	Low general/icmp	131
2.16	192.168.68.82	132
2.16.1	Low general/icmp	132
2.16.2	Low general/tcp	134
2.17	192.168.68.81	135
2.17.1	Low general/tcp	135
2.17.2	Low general/icmp	136
2.18	192.168.68.102	137
2.18.1	Low general/tcp	137
2.18.2	Low general/icmp	139
2.19	192.168.68.80	140
2.19.1	Low general/icmp	140
2.19.2	Low general/tcp	141
2.20	192.168.68.62	142
2.20.1	Low general/icmp	142
2.20.2	Low general/tcp	144
2.21	192.168.68.91	145
2.21.1	Low general/tcp	145
2.21.2	Low general/icmp	146
2.22	192.168.68.54	147
2.22.1	Low general/tcp	147
2.22.2	Low general/icmp	149
2.23	192.168.68.75	150
2.23.1	Low general/tcp	150
2.23.2	Low general/icmp	151
2.24	192.168.68.100	152
2.24.1	Low general/tcp	152
2.24.2	Low general/icmp	154

2.25	192.168.68.98	155
2.25.1	Low general/tcp	155
2.25.2	Low general/icmp	156
2.26	192.168.68.70	157
2.26.1	Low general/tcp	157
2.26.2	Low general/icmp	159
2.27	192.168.68.60	160
2.27.1	Low general/icmp	160
2.27.2	Low general/tcp	161
2.28	192.168.68.84	162
2.28.1	Low general/icmp	162
2.28.2	Low general/tcp	164
2.29	192.168.68.72	165
2.29.1	Low general/tcp	165
2.30	192.168.68.97	166
2.30.1	Low general/icmp	166

## 1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.68.110	2	4	1	0	0
192.168.71.247	0	2	2	0	0
192.168.71.250	0	1	2	0	0
192.168.71.246	0	1	2	0	0
192.168.68.1 tplinkdeco.net	0	1	2	0	0
192.168.71.248	0	1	2	0	0
192.168.71.249	0	1	2	0	0
192.168.68.106	0	1	0	0	0
192.168.68.83	0	1	0	0	0
192.168.68.87	0	5	2	0	0
192.168.68.90	0	5	2	0	0
192.168.68.56	0	5	2	0	0
192.168.68.58	0	3	2	0	0
192.168.68.86	0	0	2	0	0
192.168.68.88	0	0	2	0	0
192.168.68.82	0	0	2	0	0
192.168.68.81	0	0	2	0	0
192.168.68.102	0	0	2	0	0
192.168.68.80	0	0	2	0	0
192.168.68.62	0	0	2	0	0
192.168.68.91	0	0	2	0	0
192.168.68.54	0	0	2	0	0
192.168.68.75	0	0	2	0	0
192.168.68.100	0	0	2	0	0
192.168.68.98	0	0	2	0	0
192.168.68.70	0	0	2	0	0
192.168.68.60	0	0	2	0	0
192.168.68.84	0	0	2	0	0
192.168.68.72	0	0	1	0	0
192.168.68.97	0	0	1	0	0
Total: 30	2	31	53	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 86 results selected by the filtering described above. Before filtering there were 1457 results.

## 2 Results per Host

### 2.1 192.168.68.110

Host scan start Mon Mar 3 17:17:23 2025 UTC

Host scan end Mon Mar 3 18:02:26 2025 UTC

Service (Port)	Threat Level
<a href="#">4595/tcp</a>	High
<a href="#">4596/tcp</a>	High
<a href="#">3389/tcp</a>	Medium
<a href="#">135/tcp</a>	Medium
<a href="#">4595/tcp</a>	Medium
<a href="#">4596/tcp</a>	Medium
<a href="#">general/icmp</a>	Low

#### 2.1.1 High 4595/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\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (SWEET32)

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

... continues on next page ...

...continued from previous page ...
<b>TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)</b>
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> Services accepting vulnerable SSL/TLS cipher suites via HTTPS.
<b>Vulnerability Insight</b> 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).
<b>Vulnerability Detection Method</b> 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
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2016-2183 cve: CVE-2016-6329 cve: CVE-2020-12872 url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://mozilla.github.io/server-side-tls/ssl-config-generator/">https://mozilla.github.io/server-side-tls/ssl-config-generator/</a> url: <a href="https://sweet32.info/">https://sweet32.info/</a> 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
...continues on next page ...

...continued from previous page ...

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  
dfn-cert: DFN-CERT-2021-0770  
dfn-cert: DFN-CERT-2021-0274  
dfn-cert: DFN-CERT-2020-2141  
dfn-cert: DFN-CERT-2020-0368

...continues on next page ...



...continued from previous page ...

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  
dfn-cert: DFN-CERT-2016-1378

[\[ return to 192.168.68.110 \]](#)

## 2.1.2 High 4596/tcp

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
<b>Product detection result</b> 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)
<b>Summary</b> 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%
<b>Vulnerability Detection Result</b> 'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32) 'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32) 'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> Services accepting vulnerable SSL/TLS cipher suites via HTTPS.
<b>Vulnerability Insight</b> 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).
<b>Vulnerability Detection Method</b> 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
<b>Product Detection Result</b> 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-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

...continues on next page ...

...continued from previous page ...

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  
dfn-cert: DFN-CERT-2017-0816  
dfn-cert: DFN-CERT-2017-0746  
dfn-cert: DFN-CERT-2017-0677

...continues on next page ...

...continued from previous page ...

```

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 192.168.68.110](#) ]

### 2.1.3 Medium 3389/tcp

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 ... continues on next page ...

...continued from previous page ...
↔.25623.1.0.802067) VT.
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> 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)
<b>Vulnerability Detection Method</b> 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
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2011-3389 cve: CVE-2015-0204 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a> url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a> url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↔-report-2014 cert-bund: WID-SEC-2023-1435
... continues on next page ...

...continued from previous page ...

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  
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

...continues on next page ...

...continued from previous page ...

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  
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

...continues on next page ...



...continued from previous page ...

```
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
```

[\[ return to 192.168.68.110 \]](#)**2.1.4 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: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0

Endpoint: ncacn\_ip\_tcp:192.168.68.110[49664]

Annotation: RemoteAccessCheck

UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1

Endpoint: ncacn\_ip\_tcp:192.168.68.110[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:192.168.68.110[49664]

Annotation: Ngc Pop Key Service

UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1

Endpoint: ncacn\_ip\_tcp:192.168.68.110[49664]

Annotation: Ngc Pop Key Service

UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2

Endpoint: ncacn\_ip\_tcp:192.168.68.110[49664]

Annotation: KeyIso

Port: 49665/tcp

UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1

Endpoint: ncacn\_ip\_tcp:192.168.68.110[49665]

...continues on next page ...

...continued from previous page...	
Port: 49666/tcp	UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:192.168.68.110[49666] Annotation: Event log TCPIP
Port: 49667/tcp	UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:192.168.68.110[49667] UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:192.168.68.110[49667]
Port: 49668/tcp	UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1 Endpoint: ncacn_ip_tcp:192.168.68.110[49668]
Port: 49669/tcp	UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:192.168.68.110[49669] Annotation: RemoteAccessCheck UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1 Endpoint: ncacn_ip_tcp:192.168.68.110[49669] Annotation: Ngc Pop Key Service UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:192.168.68.110[49669] Annotation: Ngc Pop Key Service UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:192.168.68.110[49669] Annotation: KeyIso
Port: 49710/tcp	UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:192.168.68.110[49710]
Port: 49717/tcp	UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1 Endpoint: ncacn_ip_tcp:192.168.68.110[49717] Annotation: Remote Fw APIs
Note: DCE/RPC or MSRPC services running on this host locally were identified. Reporting this list is not enabled by default due to the possible large size of this list. See the script preferences to enable this reporting.	
<b>Impact</b> An attacker may use this fact to gain more knowledge about the remote host.	
<b>Solution:</b> <b>Solution type:</b> Mitigation Filter incoming traffic to this ports.	
<b>Vulnerability Detection Method</b> Details: DCE/RPC and MSRPC Services Enumeration Reporting OID:1.3.6.1.4.1.25623.1.0.10736	
...continues on next page...	

...continued from previous page ...

Version used: 2022-06-03T10:17:07Z

[\[ return to 192.168.68.110 \]](#)**2.1.5 Medium 4595/tcp**

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**

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:

... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> <li>- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)</li> <li>- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)</li> </ul>
<p><b>Vulnerability Detection Method</b></p> <p>Check the used TLS protocols of the services provided by this system.</p> <p>Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection</p> <p>OID:1.3.6.1.4.1.25623.1.0.117274</p> <p>Version used: 2024-09-27T05:05:23Z</p>
<p><b>Product Detection Result</b></p> <p>Product: cpe:/a:ietf:transport_layer_security:1.0</p> <p>Method: SSL/TLS: Version Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.105782)</p>
<p><b>References</b></p> <p>cve: CVE-2011-3389</p> <p>cve: CVE-2015-0204</p> <p>url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a></p> <p>url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a></p> <p>url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a></p> <p>url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a></p> <p>url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a></p> <p>url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a></p> <p>↔-report-2014</p> <p>cert-bund: WID-SEC-2023-1435</p> <p>cert-bund: CB-K18/0799</p> <p>cert-bund: CB-K16/1289</p> <p>cert-bund: CB-K16/1096</p> <p>cert-bund: CB-K15/1751</p> <p>cert-bund: CB-K15/1266</p> <p>cert-bund: CB-K15/0850</p> <p>cert-bund: CB-K15/0764</p> <p>cert-bund: CB-K15/0720</p> <p>cert-bund: CB-K15/0548</p> <p>cert-bund: CB-K15/0526</p> <p>cert-bund: CB-K15/0509</p> <p>cert-bund: CB-K15/0493</p> <p>cert-bund: CB-K15/0384</p> <p>cert-bund: CB-K15/0365</p> <p>cert-bund: CB-K15/0364</p> <p>cert-bund: CB-K15/0302</p> <p>cert-bund: CB-K15/0192</p> <p>cert-bund: CB-K15/0079</p> <p>cert-bund: CB-K15/0016</p> <p>cert-bund: CB-K14/1342</p>
...continues on next page ...

...continued from previous page ...

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  
 dfn-cert: DFN-CERT-2012-0848

...continues on next page ...

...continued from previous page ...

```
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
```

[\[ return to 192.168.68.110 \]](#)

### 2.1.6 Medium 4596/tcp

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)

...continues on next page ...

...continued from previous page ...
<b>Summary</b> It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
<b>Quality of Detection (QoD):</b> 98%
<b>Vulnerability Detection Result</b> 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.
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> 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)
<b>Vulnerability Detection Method</b> 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
<b>Product Detection Result</b> 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)
... continues on next page ...

...continued from previous page ...

**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  
dfn-cert: DFN-CERT-2015-1332  
dfn-cert: DFN-CERT-2015-0884  
dfn-cert: DFN-CERT-2015-0800

...continues on next page ...



...continued from previous page ...

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  
dfn-cert: DFN-CERT-2012-0142  
dfn-cert: DFN-CERT-2012-0126  
dfn-cert: DFN-CERT-2012-0123

...continues on next page ...

...continued from previous page ...

```

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

```

[\[ return to 192.168.68.110 \]](#)**2.1.7 Low general/icmp**

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**

The remote host responded to an ICMP timestamp request.

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

The following response / ICMP packet has been received:

- ICMP Type: 14
- ICMP Code: 0

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

... continues on next page ...

...continued from previous page ...

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: ICMP Timestamp Reply Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: 2025-01-21T05:37:33Z

**References**

cve: CVE-1999-0524

url: <https://datatracker.ietf.org/doc/html/rfc792>

url: <https://datatracker.ietf.org/doc/html/rfc2780>

cert-bund: CB-K15/1514

cert-bund: CB-K14/0632

dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.68.110 \]](#)

**2.2 192.168.71.247**

Host scan start Mon Mar 3 15:59:04 2025 UTC

Host scan end Mon Mar 3 17:46:17 2025 UTC

Service (Port)	Threat Level
<a href="#">443/tcp</a>	Medium
<a href="#">general/tcp</a>	Low
<a href="#">general/icmp</a>	Low

**2.2.1 Medium 443/tcp**

Medium (CVSS: 5.8)

NVT: SSL/TLS: Renegotiation MITM Vulnerability (CVE-2009-3555)

**Summary**

The remote SSL/TLS service is prone to a man-in-the-middle (MITM) vulnerability.

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

... continues on next page ...

...continued from previous page...	
<b>Vulnerability Detection Result</b> Protocol Version   Successful re-done SSL/TLS handshakes (Renegotiation) over an ⇔ existing / already established SSL/TLS connection ----- ⇔----- TLSv1.2   2	
<b>Impact</b> A remote, unauthenticated attacker may be able to inject an arbitrary amount of chosen plaintext into the beginning of the application protocol stream. This could allow and attacker to issue HTTP requests, or take action impersonating the user, among other consequences.	
<b>Solution:</b> <b>Solution type:</b> VendorFix Users should contact their vendors for specific patch information. General solution options are: - remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service - enable Safe/Secure renegotiation (RFC5746) for the affected SSL/TLS service	
<b>Affected Software/OS</b> The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products.	
<b>Vulnerability Insight</b> The flaw exists because the remote SSL/TLS service does not properly associate renegotiation handshakes with an existing connection, which allows MITM attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a 'plaintext injection' attack, aka the 'Project Mogul' issue.	
<b>Vulnerability Detection Method</b> 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 MITM Vulnerability (CVE-2009-3555) OID:1.3.6.1.4.1.25623.1.0.117758 Version used: 2024-09-27T05:05:23Z	
<b>References</b> cve: CVE-2009-3555 url: <a href="https://blog.g-sec.lu/2009/11/tls-ssl3-renegotiation-vulnerability.html">https://blog.g-sec.lu/2009/11/tls-ssl3-renegotiation-vulnerability.html</a> url: <a href="https://www.g-sec.lu/practicaltls.pdf">https://www.g-sec.lu/practicaltls.pdf</a> url: <a href="https://www.kb.cert.org/vuls/id/120541">https://www.kb.cert.org/vuls/id/120541</a> url: <a href="https://orchilles.com/ssl-renegotiation-dos/">https://orchilles.com/ssl-renegotiation-dos/</a>	
...continues on next page...	

...continued from previous page ...

url: <https://lwn.net/Articles/362234/>  
url: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD36385>  
url: <https://datatracker.ietf.org/doc/html/rfc5746>  
url: <https://mailarchive.ietf.org/arch/msg/tls/Y103HUcq9T94rMLCGPTTozURtSI/>  
cert-bund: CB-K17/1878  
cert-bund: CB-K17/1642  
cert-bund: CB-K15/0637  
dfn-cert: DFN-CERT-2017-1960  
dfn-cert: DFN-CERT-2017-1722  
dfn-cert: DFN-CERT-2015-0664  
dfn-cert: DFN-CERT-2013-0321  
dfn-cert: DFN-CERT-2012-1377  
dfn-cert: DFN-CERT-2012-0828  
dfn-cert: DFN-CERT-2012-0613  
dfn-cert: DFN-CERT-2011-1720  
dfn-cert: DFN-CERT-2011-1138  
dfn-cert: DFN-CERT-2011-1137  
dfn-cert: DFN-CERT-2011-0712  
dfn-cert: DFN-CERT-2011-0700  
dfn-cert: DFN-CERT-2011-0321  
dfn-cert: DFN-CERT-2011-0193  
dfn-cert: DFN-CERT-2011-0185  
dfn-cert: DFN-CERT-2011-0181  
dfn-cert: DFN-CERT-2011-0116  
dfn-cert: DFN-CERT-2011-0021  
dfn-cert: DFN-CERT-2011-0020  
dfn-cert: DFN-CERT-2011-0019  
dfn-cert: DFN-CERT-2010-1762  
dfn-cert: DFN-CERT-2010-1731  
dfn-cert: DFN-CERT-2010-1710  
dfn-cert: DFN-CERT-2010-1702  
dfn-cert: DFN-CERT-2010-1650  
dfn-cert: DFN-CERT-2010-1647  
dfn-cert: DFN-CERT-2010-1527  
dfn-cert: DFN-CERT-2010-1500  
dfn-cert: DFN-CERT-2010-1439  
dfn-cert: DFN-CERT-2010-1424  
dfn-cert: DFN-CERT-2010-1406  
dfn-cert: DFN-CERT-2010-1405  
dfn-cert: DFN-CERT-2010-1387  
dfn-cert: DFN-CERT-2010-1385  
dfn-cert: DFN-CERT-2010-1380  
dfn-cert: DFN-CERT-2010-1368  
dfn-cert: DFN-CERT-2010-1293  
dfn-cert: DFN-CERT-2010-1227  
dfn-cert: DFN-CERT-2010-1052  
dfn-cert: DFN-CERT-2010-1009

...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2010-1000  
dfn-cert: DFN-CERT-2010-0899  
dfn-cert: DFN-CERT-2010-0859  
dfn-cert: DFN-CERT-2010-0833  
dfn-cert: DFN-CERT-2010-0815  
dfn-cert: DFN-CERT-2010-0775  
dfn-cert: DFN-CERT-2010-0729  
dfn-cert: DFN-CERT-2010-0725  
dfn-cert: DFN-CERT-2010-0707  
dfn-cert: DFN-CERT-2010-0705  
dfn-cert: DFN-CERT-2010-0669  
dfn-cert: DFN-CERT-2010-0639  
dfn-cert: DFN-CERT-2010-0619  
dfn-cert: DFN-CERT-2010-0618  
dfn-cert: DFN-CERT-2010-0603  
dfn-cert: DFN-CERT-2010-0586  
dfn-cert: DFN-CERT-2010-0579  
dfn-cert: DFN-CERT-2010-0562  
dfn-cert: DFN-CERT-2010-0558  
dfn-cert: DFN-CERT-2010-0544  
dfn-cert: DFN-CERT-2010-0539  
dfn-cert: DFN-CERT-2010-0525  
dfn-cert: DFN-CERT-2010-0504  
dfn-cert: DFN-CERT-2010-0498  
dfn-cert: DFN-CERT-2010-0491  
dfn-cert: DFN-CERT-2010-0488  
dfn-cert: DFN-CERT-2010-0485  
dfn-cert: DFN-CERT-2010-0456  
dfn-cert: DFN-CERT-2010-0455  
dfn-cert: DFN-CERT-2010-0451  
dfn-cert: DFN-CERT-2010-0413  
dfn-cert: DFN-CERT-2010-0411  
dfn-cert: DFN-CERT-2010-0410  
dfn-cert: DFN-CERT-2010-0407  
dfn-cert: DFN-CERT-2010-0406  
dfn-cert: DFN-CERT-2010-0405  
dfn-cert: DFN-CERT-2010-0388  
dfn-cert: DFN-CERT-2010-0370  
dfn-cert: DFN-CERT-2010-0339  
dfn-cert: DFN-CERT-2010-0303  
dfn-cert: DFN-CERT-2010-0273  
dfn-cert: DFN-CERT-2010-0201  
dfn-cert: DFN-CERT-2010-0166  
dfn-cert: DFN-CERT-2010-0050  
dfn-cert: DFN-CERT-2010-0030  
dfn-cert: DFN-CERT-2009-1833  
dfn-cert: DFN-CERT-2009-1821

...continues on next page ...

...continued from previous page ...

```

dfn-cert: DFN-CERT-2009-1820
dfn-cert: DFN-CERT-2009-1809
dfn-cert: DFN-CERT-2009-1805
dfn-cert: DFN-CERT-2009-1757
dfn-cert: DFN-CERT-2009-1755
dfn-cert: DFN-CERT-2009-1725
dfn-cert: DFN-CERT-2009-1719
dfn-cert: DFN-CERT-2009-1689
dfn-cert: DFN-CERT-2009-1688
dfn-cert: DFN-CERT-2009-1654
dfn-cert: DFN-CERT-2009-1653
dfn-cert: DFN-CERT-2009-1646
dfn-cert: DFN-CERT-2009-1643
dfn-cert: DFN-CERT-2009-1630
dfn-cert: DFN-CERT-2009-1623
dfn-cert: DFN-CERT-2009-1603
dfn-cert: DFN-CERT-2009-1602
dfn-cert: DFN-CERT-2009-1584
dfn-cert: DFN-CERT-2009-1578

```

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.

... continues on next page ...

...continued from previous page ...
<b>Affected Software/OS</b> Every SSL/TLS service which does not properly restrict client-initiated renegotiation.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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
<b>References</b> cve: CVE-2011-1473 cve: CVE-2011-5094 url: <a href="https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/">https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</a> url: <a href="https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/">https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</a> url: <a href="https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation">https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</a> url: <a href="https://www.openwall.com/lists/oss-security/2011/07/08/2">https://www.openwall.com/lists/oss-security/2011/07/08/2</a> 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

[\[ return to 192.168.71.247 \]](#)

2.2.2 Low general/tcp



Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 11838891 Packet 2: 11839104
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b> <b>Solution type:</b> Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d</a> ... continues on next page ...

...continued from previous page ...

↩️ownload/details.aspx?id=9152

url: https://www.fortiguard.com/psirt/FG-IR-16-090

[\[ return to 192.168.71.247 \]](#)**2.2.3 Low general/icmp**

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**

The remote host responded to an ICMP timestamp request.

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

The following response / ICMP packet has been received:

- ICMP Type: 14
- ICMP Code: 0

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: ICMP Timestamp Reply Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: 2025-01-21T05:37:33Z

... continues on next page ...

...continued from previous page ...	
<b>References</b> cve: CVE-1999-0524 url: https://datatracker.ietf.org/doc/html/rfc792 url: https://datatracker.ietf.org/doc/html/rfc2780 cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658	

[ [return to 192.168.71.247](#) ]

2.3 192.168.71.250

Host scan start Mon Mar 3 15:59:04 2025 UTC  
Host scan end Mon Mar 3 17:46:14 2025 UTC

Service (Port)	Threat Level
<a href="#">443/tcp</a>	Medium
<a href="#">general/icmp</a>	Low
<a href="#">general/tcp</a>	Low

2.3.1 Medium 443/tcp

Medium (CVSS: 5.0) NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
<b>Summary</b> The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.
<b>Quality of Detection (QoD):</b> 70%
<b>Vulnerability Detection Result</b> 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 ----- ↪----- TLShv1.2   10
<b>Impact</b> The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.
<b>Solution:</b>
... continues on next page ...

...continued from previous page ...	
<b>Solution type:</b> 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.
<b>Affected Software/OS</b>	Every SSL/TLS service which does not properly restrict client-initiated renegotiation.
<b>Vulnerability Insight</b>	<p>The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.</p> <p>Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:</p> <p>&gt; 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.</p> <p>Both CVEs are still kept in this VT as a reference to the origin of this flaw.</p>
<b>Vulnerability Detection Method</b>	<p>Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.</p> <p>Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)</p> <p>OID:1.3.6.1.4.1.25623.1.0.117761</p> <p>Version used: 2024-09-27T05:05:23Z</p>
<b>References</b>	<p>cve: CVE-2011-1473</p> <p>cve: CVE-2011-5094</p> <p>url: <a href="https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/">https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</a></p> <p>url: <a href="https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/">https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</a></p> <p>url: <a href="https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation">https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</a></p> <p>url: <a href="https://www.openwall.com/lists/oss-security/2011/07/08/2">https://www.openwall.com/lists/oss-security/2011/07/08/2</a></p> <p>cert-bund: WID-SEC-2024-1591</p> <p>cert-bund: WID-SEC-2024-0796</p> <p>cert-bund: WID-SEC-2023-1435</p> <p>cert-bund: CB-K17/0980</p> <p>cert-bund: CB-K17/0979</p> <p>cert-bund: CB-K14/0772</p> <p>cert-bund: CB-K13/0915</p> <p>cert-bund: CB-K13/0462</p> <p>dfn-cert: DFN-CERT-2017-1013</p> <p>dfn-cert: DFN-CERT-2017-1012</p> <p>dfn-cert: DFN-CERT-2014-0809</p> <p>dfn-cert: DFN-CERT-2013-1928</p> <p>dfn-cert: DFN-CERT-2012-1112</p>

[\[ return to 192.168.71.250 \]](#)

## 2.3.2 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: - ICMP Type: 14 - ICMP Code: 0
<b>Impact</b> This information could theoretically be used to exploit weak time-based random number generators in other services.
<b>Solution:</b> <b>Solution type:</b> Mitigation Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)
<b>Vulnerability Insight</b> The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.
<b>Vulnerability Detection Method</b> Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2025-01-21T05:37:33Z
<b>References</b> cve: CVE-1999-0524 url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a> cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.71.250 \]](#)

### 2.3.3 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 1525601409 Packet 2: 1525604064
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b> <b>Solution type:</b> Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
...
... continues on next page ...

...continued from previous page ...
<b>References</b> url: https://datatracker.ietf.org/doc/html/rfc1323 url: https://datatracker.ietf.org/doc/html/rfc7323 url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152 url: https://www.fortiguard.com/psirt/FG-IR-16-090

[ [return to 192.168.71.250](#) ]

2.4 192.168.71.246

Host scan start Mon Mar 3 15:59:04 2025 UTC  
Host scan end Mon Mar 3 17:47:53 2025 UTC

Service (Port)	Threat Level
<a href="#">443/tcp</a>	Medium
<a href="#">general/tcp</a>	Low
<a href="#">general/icmp</a>	Low

2.4.1 Medium 443/tcp

Medium (CVSS: 5.0) NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
<b>Summary</b> The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.
<b>Quality of Detection (QoD):</b> 70%
<b>Vulnerability Detection Result</b> 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
<b>Impact</b> The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.
<b>Solution:</b> <b>Solution type:</b> VendorFix
... continues on next page ...

<p>...continued from previous page ...</p> <p>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.</p>
<p><b>Affected Software/OS</b> Every SSL/TLS service which does not properly restrict client-initiated renegotiation.</p>
<p><b>Vulnerability Insight</b> 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: &gt; 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.</p>
<p><b>Vulnerability Detection Method</b> 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</p>
<p><b>References</b> cve: CVE-2011-1473 cve: CVE-2011-5094 url: <a href="https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/">https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</a> url: <a href="https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/">https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</a> url: <a href="https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation">https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</a> url: <a href="https://www.openwall.com/lists/oss-security/2011/07/08/2">https://www.openwall.com/lists/oss-security/2011/07/08/2</a> 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</p>



## 2.4.2 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 11851424 Packet 2: 11851538
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b> <b>Solution type:</b> Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> ... continues on next page ...

...continued from previous page ...
url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a>
url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a>
url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a>

[\[ return to 192.168.71.246 \]](#)

### 2.4.3 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: <ul style="list-style-type: none"> <li>- ICMP Type: 14</li> <li>- ICMP Code: 0</li> </ul>
<b>Impact</b> This information could theoretically be used to exploit weak time-based random number generators in other services.
<b>Solution:</b> <b>Solution type:</b> Mitigation Various mitigations are possible: <ul style="list-style-type: none"> <li>- Disable the support for ICMP timestamp on the remote host completely</li> <li>- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)</li> </ul>
<b>Vulnerability Insight</b> The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.
<b>Vulnerability Detection Method</b> Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190
... continues on next page ...

...continued from previous page ...
Version used: 2025-01-21T05:37:33Z
<b>References</b> cve: CVE-1999-0524 url: https://datatracker.ietf.org/doc/html/rfc792 url: https://datatracker.ietf.org/doc/html/rfc2780 cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658

[ [return to 192.168.71.246](#) ]

2.5 192.168.68.1

Host scan start Mon Mar 3 16:08:51 2025 UTC  
Host scan end Mon Mar 3 17:55:33 2025 UTC

Service (Port)	Threat Level
<a href="#">443/tcp</a>	Medium
<a href="#">general/tcp</a>	Low
<a href="#">general/icmp</a>	Low

2.5.1 Medium 443/tcp

Medium (CVSS: 5.0) NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
<b>Summary</b> The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.
<b>Quality of Detection (QoD):</b> 70%
<b>Vulnerability Detection Result</b> 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
<b>Impact</b> 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 ...
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> Every SSL/TLS service which does not properly restrict client-initiated renegotiation.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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
<b>References</b> cve: CVE-2011-1473 cve: CVE-2011-5094 url: <a href="https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/">https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</a> url: <a href="https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/">https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</a> url: <a href="https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation">https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</a> url: <a href="https://www.openwall.com/lists/oss-security/2011/07/08/2">https://www.openwall.com/lists/oss-security/2011/07/08/2</a> 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

[\[ return to 192.168.68.1 \]](#)**2.5.2 Low general/tcp**

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

**Summary**

The remote host implements TCP timestamps and therefore allows to compute the uptime.

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

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:

Packet 1: 1622831304

Packet 2: 1622833107

**Impact**

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

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

To disable TCP timestamps on linux add the line 'net.ipv4.tcp\_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

**Affected Software/OS**

TCP implementations that implement RFC1323/RFC7323.

**Vulnerability Insight**

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

**Vulnerability Detection Method**

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

... continues on next page ...

...continued from previous page ...
Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a> url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a>

[\[ return to 192.168.68.1 \]](#)

### 2.5.3 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: <ul style="list-style-type: none"> <li>- ICMP Type: 14</li> <li>- ICMP Code: 0</li> </ul>
<b>Impact</b> This information could theoretically be used to exploit weak time-based random number generators in other services.
<b>Solution:</b> <b>Solution type:</b> Mitigation Various mitigations are possible: <ul style="list-style-type: none"> <li>- Disable the support for ICMP timestamp on the remote host completely</li> <li>- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)</li> </ul>
<b>Vulnerability Insight</b> The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.
... continues on next page ...

...continued from previous page ...

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: ICMP Timestamp Reply Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: 2025-01-21T05:37:33Z

**References**

cve: CVE-1999-0524

url: <https://datatracker.ietf.org/doc/html/rfc792>

url: <https://datatracker.ietf.org/doc/html/rfc2780>

cert-bund: CB-K15/1514

cert-bund: CB-K14/0632

dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.68.1 \]](#)

**2.6 192.168.71.248**

Host scan start Mon Mar 3 15:59:04 2025 UTC

Host scan end Mon Mar 3 17:45:29 2025 UTC

Service (Port)	Threat Level
<a href="#">443/tcp</a>	Medium
<a href="#">general/icmp</a>	Low
<a href="#">general/tcp</a>	Low

**2.6.1 Medium 443/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
<b>Impact</b> The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.	
<b>Solution:</b> <b>Solution type:</b> 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.	
<b>Affected Software/OS</b> Every SSL/TLS service which does not properly restrict client-initiated renegotiation.	
<b>Vulnerability Insight</b> 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.	
<b>Vulnerability Detection Method</b> 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	
<b>References</b> cve: CVE-2011-1473 cve: CVE-2011-5094 url: <a href="https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/">https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</a> url: <a href="https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/">https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</a> url: <a href="https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation">https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</a> url: <a href="https://www.openwall.com/lists/oss-security/2011/07/08/2">https://www.openwall.com/lists/oss-security/2011/07/08/2</a> 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	
... continues on next page ...	



...continued from previous page ...

```

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 192.168.71.248](#) ]**2.6.2 Low general/icmp**

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**

The remote host responded to an ICMP timestamp request.

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

The following response / ICMP packet has been received:

- ICMP Type: 14
- ICMP Code: 0

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

... continues on next page ...

...continued from previous page ...
<p>Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.</p> <p>Details: ICMP Timestamp Reply Information Disclosure</p> <p>OID:1.3.6.1.4.1.25623.1.0.103190</p> <p>Version used: 2025-01-21T05:37:33Z</p>
<p><b>References</b></p> <p>cve: CVE-1999-0524</p> <p>url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a></p> <p>url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a></p> <p>cert-bund: CB-K15/1514</p> <p>cert-bund: CB-K14/0632</p> <p>dfn-cert: DFN-CERT-2014-0658</p>

[ [return to 192.168.71.248](#) ]

### 2.6.3 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<p><b>Summary</b></p> <p>The remote host implements TCP timestamps and therefore allows to compute the uptime.</p>
<p><b>Quality of Detection (QoD):</b> 80%</p>
<p><b>Vulnerability Detection Result</b></p> <p>It was detected that the host implements RFC1323/RFC7323.</p> <p>The following timestamps were retrieved with a delay of 1 seconds in-between:</p> <p>Packet 1: 852791394</p> <p>Packet 2: 852793061</p>
<p><b>Impact</b></p> <p>A side effect of this feature is that the uptime of the remote host can sometimes be computed.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.</p> <p>To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'</p> <p>Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.</p> <p>The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.</p>
... continues on next page ...

...continued from previous page ...
See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a> url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a>

[ [return to 192.168.71.248](#) ]

2.7 192.168.71.249

Host scan start Mon Mar 3 15:59:04 2025 UTC  
Host scan end Mon Mar 3 17:49:13 2025 UTC

Service (Port)	Threat Level
<a href="#">443/tcp</a>	Medium
<a href="#">general/icmp</a>	Low
<a href="#">general/tcp</a>	Low

2.7.1 Medium 443/tcp

Medium (CVSS: 5.0) NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
<b>Summary</b> The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.
... continues on next page ...

...continued from previous page...
<b>Quality of Detection (QoD):</b> 70%
<b>Vulnerability Detection Result</b> 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
<b>Impact</b> The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> Every SSL/TLS service which does not properly restrict client-initiated renegotiation.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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
<b>References</b> cve: CVE-2011-1473 cve: CVE-2011-5094 url: <a href="https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/">https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</a> url: <a href="https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/">https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</a>
...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 192.168.71.249](#) ]

2.7.2 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: - ICMP Type: 14 - ICMP Code: 0
<b>Impact</b> This information could theoretically be used to exploit weak time-based random number generators in other services.
<b>Solution:</b> <b>Solution type:</b> Mitigation Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)
... continues on next page ...

...continued from previous page ...

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: ICMP Timestamp Reply Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: 2025-01-21T05:37:33Z

**References**

cve: CVE-1999-0524

url: <https://datatracker.ietf.org/doc/html/rfc792>

url: <https://datatracker.ietf.org/doc/html/rfc2780>

cert-bund: CB-K15/1514

cert-bund: CB-K14/0632

dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.71.249 \]](#)

**2.7.3 Low general/tcp**

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

**Summary**

The remote host implements TCP timestamps and therefore allows to compute the uptime.

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

**Vulnerability Detection Result**

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:

Packet 1: 11864850

Packet 2: 11865151

**Impact**

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

**Solution:**

**Solution type:** Mitigation

... continues on next page ...

...continued from previous page ...
<p>To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.</p> <p>To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.</p> <p>See the references for more information.</p>
<p><b>Affected Software/OS</b></p> <p>TCP implementations that implement RFC1323/RFC7323.</p>
<p><b>Vulnerability Insight</b></p> <p>The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.</p> <p>Details: TCP Timestamps Information Disclosure</p> <p>OID:1.3.6.1.4.1.25623.1.0.80091</p> <p>Version used: 2023-12-15T16:10:08Z</p>
<p><b>References</b></p> <p>url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a></p> <p>url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a></p> <p>url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a></p> <p>url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a></p>

[ [return to 192.168.71.249](#) ]

## 2.8 192.168.68.106

Host scan start Mon Mar 3 16:20:38 2025 UTC

Host scan end Mon Mar 3 17:08:25 2025 UTC

Service (Port)	Threat Level
<a href="#">135/tcp</a>	Medium

### 2.8.1 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: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0

Endpoint: ncacn\_ip\_tcp:192.168.68.106[49664]

Annotation: RemoteAccessCheck

UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1

Endpoint: ncacn\_ip\_tcp:192.168.68.106[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:192.168.68.106[49664]

Annotation: Ngc Pop Key Service

UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1

Endpoint: ncacn\_ip\_tcp:192.168.68.106[49664]

Annotation: Ngc Pop Key Service

UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2

Endpoint: ncacn\_ip\_tcp:192.168.68.106[49664]

Annotation: KeyIso

Port: 49665/tcp

UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1

Endpoint: ncacn\_ip\_tcp:192.168.68.106[49665]

Port: 49666/tcp

UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1

Endpoint: ncacn\_ip\_tcp:192.168.68.106[49666]

Annotation: Event log TCPIP

Port: 49667/tcp

UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1

Endpoint: ncacn\_ip\_tcp:192.168.68.106[49667]

UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1

Endpoint: ncacn\_ip\_tcp:192.168.68.106[49667]

Port: 49668/tcp

UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1

Endpoint: ncacn\_ip\_tcp:192.168.68.106[49668]

Port: 49669/tcp

... continues on next page ...



...continued from previous page...	
<pre> UUID: 0b6edbf8-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:192.168.68.106[49669] UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:192.168.68.106[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:192.168.68.106[49669] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:192.168.68.106[49669] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:192.168.68.106[49669] Port: 49670/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:192.168.68.106[49670] Annotation: RemoteAccessCheck Port: 49673/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:192.168.68.106[49673] 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. </pre>	
<b>Impact</b>	An attacker may use this fact to gain more knowledge about the remote host.
<b>Solution:</b>	
<b>Solution type:</b> Mitigation	
Filter incoming traffic to this ports.	
<b>Vulnerability Detection Method</b>	
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	

[\[ return to 192.168.68.106 \]](#)

## 2.9 192.168.68.83

Host scan start Mon Mar 3 16:26:45 2025 UTC  
Host scan end Mon Mar 3 17:55:44 2025 UTC

Service (Port)	Threat Level
<a href="#">443/tcp</a>	Medium

**2.9.1 Medium 443/tcp**

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
<b>Product detection result</b> 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)
<b>Summary</b> It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
<b>Quality of Detection (QoD): 98%</b>
<b>Vulnerability Detection Result</b> 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.
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> 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)
<b>Vulnerability Detection Method</b> Check the used TLS protocols of the services provided by this system. ... continues on next page ...

...continued from previous page ...
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
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2011-3389 cve: CVE-2015-0204 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a> url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a> url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↔-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
...continues on next page ...

...continued from previous page ...	
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
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
...continues on next page ...	

...continued from previous page ...

```
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
```

[\[ return to 192.168.68.83 \]](#)

## 2.10 192.168.68.87

Host scan start Mon Mar 3 15:59:01 2025 UTC  
Host scan end Mon Mar 3 16:31:53 2025 UTC

Service (Port)	Threat Level
<a href="#">9000/tcp</a>	Medium
<a href="#">10101/tcp</a>	Medium
<a href="#">8009/tcp</a>	Medium
<a href="#">8443/tcp</a>	Medium
<a href="#">10001/tcp</a>	Medium
<a href="#">general/icmp</a>	Low
<a href="#">general/tcp</a>	Low

### 2.10.1 Medium 9000/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
<b>Product detection result</b> 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)
<b>Summary</b> It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
<b>Quality of Detection (QoD): 98%</b>
<b>Vulnerability Detection Result</b> 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.
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> 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)
<b>Vulnerability Detection Method</b> 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
... continues on next page ...

...continued from previous page ...
Version used: 2024-09-27T05:05:23Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2011-3389 cve: CVE-2015-0204 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a> url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a> url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↔-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
...continues on next page ...

...continued from previous page ...

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  
dfn-cert: DFN-CERT-2012-0354

...continues on next page ...



...continued from previous page ...

```

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

```

[\[ return to 192.168.68.87 \]](#)

### 2.10.2 Medium 10101/tcp

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

... continues on next page ...

...continued from previous page ...
<p>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.</p>
<p><b>Impact</b></p> <p>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.</p> <p>Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>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.</p>
<p><b>Affected Software/OS</b></p> <p>All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.</p>
<p><b>Vulnerability Insight</b></p> <p>The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:</p> <ul style="list-style-type: none"> <li>- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)</li> <li>- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)</li> </ul>
<p><b>Vulnerability Detection Method</b></p> <p>Check the used TLS protocols of the services provided by this system.</p> <p>Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.117274</p> <p>Version used: 2024-09-27T05:05:23Z</p>
<p><b>Product Detection Result</b></p> <p>Product: cpe:/a:ietf:transport_layer_security:1.0</p> <p>Method: SSL/TLS: Version Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.105782)</p>
<p><b>References</b></p> <p>cve: CVE-2011-3389</p> <p>cve: CVE-2015-0204</p> <p>url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a></p> <p>url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a></p> <p>url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a></p> <p>url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a></p> <p>url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a></p>
... continues on next page ...

...continued from previous page ...

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

dfn-cert: DFN-CERT-2015-0374

dfn-cert: DFN-CERT-2015-0305

... continues on next page ...

...continued from previous page ...

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  
dfn-cert: DFN-CERT-2011-1844  
dfn-cert: DFN-CERT-2011-1826

...continues on next page ...

...continued from previous page ...

```
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 192.168.68.87](#) ]**2.10.3 Medium 8009/tcp**

Medium (CVSS: 4.3)

NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**

cpe:/a:ietf:transport\_layer\_security:1.3

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.

... continues on next page ...

...continued from previous page ...
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> 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)
<b>Vulnerability Detection Method</b> 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
<b>Product Detection Result</b> Product: cpe:/a:ietf:transport_layer_security:1.3 Method: SSL/TLS: Version Detection OID: 1.3.6.1.4.1.25623.1.0.105782)
<b>References</b> cve: CVE-2011-3389 cve: CVE-2015-0204 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a> url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a> url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↔-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
```

[\[ return to 192.168.68.87 \]](#)

#### 2.10.4 Medium 8443/tcp



Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
<b>Product detection result</b> 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)
<b>Summary</b> It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
<b>Quality of Detection (QoD): 98%</b>
<b>Vulnerability Detection Result</b> 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.
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> 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)
<b>Vulnerability Detection Method</b> 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
... continues on next page ...

...continued from previous page ...
Version used: 2024-09-27T05:05:23Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2011-3389 cve: CVE-2015-0204 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a> url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a> url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↔-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
...continues on next page ...

...continued from previous page ...

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  
dfn-cert: DFN-CERT-2012-0354

...continues on next page ...

...continued from previous page ...

```

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

```

[\[ return to 192.168.68.87 \]](#)

### 2.10.5 Medium 10001/tcp

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

... continues on next page ...

...continued from previous page ...
<p>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.</p>
<p><b>Impact</b></p> <p>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.</p> <p>Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>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.</p>
<p><b>Affected Software/OS</b></p> <p>All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.</p>
<p><b>Vulnerability Insight</b></p> <p>The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:</p> <ul style="list-style-type: none"> <li>- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)</li> <li>- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)</li> </ul>
<p><b>Vulnerability Detection Method</b></p> <p>Check the used TLS protocols of the services provided by this system.</p> <p>Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection</p> <p>OID:1.3.6.1.4.1.25623.1.0.117274</p> <p>Version used: 2024-09-27T05:05:23Z</p>
<p><b>Product Detection Result</b></p> <p>Product: cpe:/a:ietf:transport_layer_security:1.0</p> <p>Method: SSL/TLS: Version Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.105782)</p>
<p><b>References</b></p> <p>cve: CVE-2011-3389</p> <p>cve: CVE-2015-0204</p> <p>url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a></p> <p>url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a></p> <p>url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a></p> <p>url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a></p> <p>url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a></p>
... continues on next page ...

...continued from previous page ...	
url:	<a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a>
↔-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
dfn-cert:	DFN-CERT-2015-0374
dfn-cert:	DFN-CERT-2015-0305
... continues on next page ...	

...continued from previous page ...

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  
dfn-cert: DFN-CERT-2011-1844  
dfn-cert: DFN-CERT-2011-1826

...continues on next page ...

...continued from previous page ...

```
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 192.168.68.87](#) ]**2.10.6 Low general/icmp**

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**

The remote host responded to an ICMP timestamp request.

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

The following response / ICMP packet has been received:

- ICMP Type: 14
- ICMP Code: 0

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

... continues on next page ...



...continued from previous page ...
<p>Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.</p> <p>Details: ICMP Timestamp Reply Information Disclosure</p> <p>OID:1.3.6.1.4.1.25623.1.0.103190</p> <p>Version used: 2025-01-21T05:37:33Z</p>
<p><b>References</b></p> <p>cve: CVE-1999-0524</p> <p>url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a></p> <p>url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a></p> <p>cert-bund: CB-K15/1514</p> <p>cert-bund: CB-K14/0632</p> <p>dfn-cert: DFN-CERT-2014-0658</p>

[ [return to 192.168.68.87](#) ]

### 2.10.7 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<p><b>Summary</b></p> <p>The remote host implements TCP timestamps and therefore allows to compute the uptime.</p>
<p><b>Quality of Detection (QoD):</b> 80%</p>
<p><b>Vulnerability Detection Result</b></p> <p>It was detected that the host implements RFC1323/RFC7323.</p> <p>The following timestamps were retrieved with a delay of 1 seconds in-between:</p> <p>Packet 1: 3075516</p> <p>Packet 2: 3075656</p>
<p><b>Impact</b></p> <p>A side effect of this feature is that the uptime of the remote host can sometimes be computed.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.</p> <p>To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'</p> <p>Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.</p>
... continues on next page ...

...continued from previous page ...
See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a> url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a>

[ [return to 192.168.68.87](#) ]

## 2.11 192.168.68.90

Host scan start Mon Mar 3 15:59:04 2025 UTC  
Host scan end Mon Mar 3 16:30:46 2025 UTC

Service (Port)	Threat Level
<a href="#">10101/tcp</a>	Medium
<a href="#">8443/tcp</a>	Medium
<a href="#">8009/tcp</a>	Medium
<a href="#">10001/tcp</a>	Medium
<a href="#">9000/tcp</a>	Medium
<a href="#">general/tcp</a>	Low
<a href="#">general/icmp</a>	Low

### 2.11.1 Medium 10101/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
<b>Product detection result</b> 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)
<b>Summary</b> It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
<b>Quality of Detection (QoD): 98%</b>
<b>Vulnerability Detection Result</b> 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.
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> 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)
<b>Vulnerability Detection Method</b> 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
... continues on next page ...

...continued from previous page ...
Version used: 2024-09-27T05:05:23Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2011-3389 cve: CVE-2015-0204 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a> url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a> url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↔-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
...continues on next page ...

...continued from previous page ...

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  
dfn-cert: DFN-CERT-2012-0354

...continues on next page ...

...continued from previous page ...

```

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

```

[\[ return to 192.168.68.90 \]](#)

### 2.11.2 Medium 8443/tcp

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

... continues on next page ...

...continued from previous page ...
<p>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.</p>
<p><b>Impact</b></p> <p>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.</p> <p>Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>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.</p>
<p><b>Affected Software/OS</b></p> <p>All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.</p>
<p><b>Vulnerability Insight</b></p> <p>The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:</p> <ul style="list-style-type: none"> <li>- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)</li> <li>- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)</li> </ul>
<p><b>Vulnerability Detection Method</b></p> <p>Check the used TLS protocols of the services provided by this system.</p> <p>Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.117274</p> <p>Version used: 2024-09-27T05:05:23Z</p>
<p><b>Product Detection Result</b></p> <p>Product: cpe:/a:ietf:transport_layer_security:1.0</p> <p>Method: SSL/TLS: Version Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.105782)</p>
<p><b>References</b></p> <p>cve: CVE-2011-3389</p> <p>cve: CVE-2015-0204</p> <p>url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a></p> <p>url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a></p> <p>url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a></p> <p>url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a></p> <p>url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a></p>
... continues on next page ...

...continued from previous page ...

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

dfn-cert: DFN-CERT-2015-0374

dfn-cert: DFN-CERT-2015-0305

... continues on next page ...



...continued from previous page ...

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  
dfn-cert: DFN-CERT-2011-1844  
dfn-cert: DFN-CERT-2011-1826

...continues on next page ...

...continued from previous page ...

```
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 192.168.68.90](#) ]**2.11.3 Medium 8009/tcp**

Medium (CVSS: 4.3)

NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Product detection result**

cpe:/a:ietf:transport\_layer\_security:1.3

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.

... continues on next page ...

...continued from previous page ...
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> 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)
<b>Vulnerability Detection Method</b> 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
<b>Product Detection Result</b> Product: cpe:/a:ietf:transport_layer_security:1.3 Method: SSL/TLS: Version Detection OID: 1.3.6.1.4.1.25623.1.0.105782)
<b>References</b> cve: CVE-2011-3389 cve: CVE-2015-0204 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a> url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a> url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↔-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
```

[\[ return to 192.168.68.90 \]](#)

#### 2.11.4 Medium 10001/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
<b>Product detection result</b> 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)
<b>Summary</b> It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
<b>Quality of Detection (QoD):</b> 98%
<b>Vulnerability Detection Result</b> 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.
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> 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)
<b>Vulnerability Detection Method</b> 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
... continues on next page ...

...continued from previous page ...
Version used: 2024-09-27T05:05:23Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2011-3389 cve: CVE-2015-0204 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a> url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a> url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↔-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
...continues on next page ...

...continued from previous page ...

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  
dfn-cert: DFN-CERT-2012-0354

...continues on next page ...



...continued from previous page ...

```

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

```

[\[ return to 192.168.68.90 \]](#)

### 2.11.5 Medium 9000/tcp

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

... continues on next page ...

...continued from previous page ...
<p>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.</p>
<p><b>Impact</b></p> <p>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.</p> <p>Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>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.</p>
<p><b>Affected Software/OS</b></p> <p>All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.</p>
<p><b>Vulnerability Insight</b></p> <p>The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:</p> <ul style="list-style-type: none"> <li>- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)</li> <li>- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)</li> </ul>
<p><b>Vulnerability Detection Method</b></p> <p>Check the used TLS protocols of the services provided by this system.</p> <p>Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection</p> <p>OID:1.3.6.1.4.1.25623.1.0.117274</p> <p>Version used: 2024-09-27T05:05:23Z</p>
<p><b>Product Detection Result</b></p> <p>Product: cpe:/a:ietf:transport_layer_security:1.0</p> <p>Method: SSL/TLS: Version Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.105782)</p>
<p><b>References</b></p> <p>cve: CVE-2011-3389</p> <p>cve: CVE-2015-0204</p> <p>url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a></p> <p>url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a></p> <p>url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a></p> <p>url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a></p> <p>url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a></p>
... continues on next page ...

...continued from previous page ...

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

dfn-cert: DFN-CERT-2015-0374

dfn-cert: DFN-CERT-2015-0305

... continues on next page ...

...continued from previous page ...

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  
dfn-cert: DFN-CERT-2011-1844  
dfn-cert: DFN-CERT-2011-1826

...continues on next page ...

...continued from previous page ...

```
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
```

[\[ return to 192.168.68.90 \]](#)**2.11.6 Low general/tcp**

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

**Summary**

The remote host implements TCP timestamps and therefore allows to compute the uptime.

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

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:

Packet 1: 19993762

Packet 2: 19994035

**Impact**

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

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

To disable TCP timestamps on linux add the line 'net.ipv4.tcp\_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

**Affected Software/OS**

TCP implementations that implement RFC1323/RFC7323.

... continues on next page ...

...continued from previous page ...
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a> url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a>

[\[ return to 192.168.68.90 \]](#)

### 2.11.7 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: - ICMP Type: 14 - ICMP Code: 0
<b>Impact</b> This information could theoretically be used to exploit weak time-based random number generators in other services.
<b>Solution:</b> <b>Solution type:</b> Mitigation Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely
... continues on next page ...

...continued from previous page ...

- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

### Vulnerability Insight

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

### Vulnerability Detection Method

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: ICMP Timestamp Reply Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: 2025-01-21T05:37:33Z

### References

cve: CVE-1999-0524

url: <https://datatracker.ietf.org/doc/html/rfc792>

url: <https://datatracker.ietf.org/doc/html/rfc2780>

cert-bund: CB-K15/1514

cert-bund: CB-K14/0632

dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.68.90 \]](#)

## 2.12 192.168.68.56

Host scan start Mon Mar 3 15:59:07 2025 UTC

Host scan end Mon Mar 3 16:37:45 2025 UTC

Service (Port)	Threat Level
<a href="#">9000/tcp</a>	Medium
<a href="#">10101/tcp</a>	Medium
<a href="#">8443/tcp</a>	Medium
<a href="#">10001/tcp</a>	Medium
<a href="#">8009/tcp</a>	Medium
<a href="#">general/icmp</a>	Low
<a href="#">general/tcp</a>	Low

### 2.12.1 Medium 9000/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
<b>Product detection result</b> 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)
<b>Summary</b> It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
<b>Quality of Detection (QoD): 98%</b>
<b>Vulnerability Detection Result</b> 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.
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> 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)
<b>Vulnerability Detection Method</b> 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
... continues on next page ...



...continued from previous page ...
Version used: 2024-09-27T05:05:23Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2011-3389 cve: CVE-2015-0204 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a> url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a> url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↔-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
...continues on next page ...

...continued from previous page ...

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  
dfn-cert: DFN-CERT-2012-0354

...continues on next page ...

...continued from previous page ...

```

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

```

[\[ return to 192.168.68.56 \]](#)

### 2.12.2 Medium 10101/tcp

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

... continues on next page ...

...continued from previous page ...
<p>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.</p>
<p><b>Impact</b></p> <p>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.</p> <p>Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>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.</p>
<p><b>Affected Software/OS</b></p> <p>All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.</p>
<p><b>Vulnerability Insight</b></p> <p>The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:</p> <ul style="list-style-type: none"> <li>- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)</li> <li>- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)</li> </ul>
<p><b>Vulnerability Detection Method</b></p> <p>Check the used TLS protocols of the services provided by this system.</p> <p>Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection</p> <p>OID:1.3.6.1.4.1.25623.1.0.117274</p> <p>Version used: 2024-09-27T05:05:23Z</p>
<p><b>Product Detection Result</b></p> <p>Product: cpe:/a:ietf:transport_layer_security:1.0</p> <p>Method: SSL/TLS: Version Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.105782)</p>
<p><b>References</b></p> <p>cve: CVE-2011-3389</p> <p>cve: CVE-2015-0204</p> <p>url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a></p> <p>url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a></p> <p>url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a></p> <p>url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a></p> <p>url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a></p>
... continues on next page ...

...continued from previous page ...

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

dfn-cert: DFN-CERT-2015-0374

dfn-cert: DFN-CERT-2015-0305

... continues on next page ...

...continued from previous page ...

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  
dfn-cert: DFN-CERT-2011-1844  
dfn-cert: DFN-CERT-2011-1826

...continues on next page ...

...continued from previous page ...

```
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
```

[\[ return to 192.168.68.56 \]](#)

### 2.12.3 Medium 8443/tcp

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.

... continues on next page ...

...continued from previous page ...
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> 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)
<b>Vulnerability Detection Method</b> 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
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2011-3389 cve: CVE-2015-0204 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a> url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a> url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↔-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
```

[\[ return to 192.168.68.56 \]](#)

#### 2.12.4 Medium 10001/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
<b>Product detection result</b> 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)
<b>Summary</b> It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
<b>Quality of Detection (QoD):</b> 98%
<b>Vulnerability Detection Result</b> 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.
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
<b>Vulnerability Insight</b> 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)
<b>Vulnerability Detection Method</b> 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
... continues on next page ...

...continued from previous page ...
Version used: 2024-09-27T05:05:23Z
<b>Product Detection Result</b> 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)
<b>References</b> cve: CVE-2011-3389 cve: CVE-2015-0204 url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a> url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a> url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a> url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a> url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a> ↔-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
...continues on next page ...

...continued from previous page ...

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  
dfn-cert: DFN-CERT-2012-0354

...continues on next page ...

...continued from previous page ...

```

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

```

[\[ return to 192.168.68.56 \]](#)

### 2.12.5 Medium 8009/tcp

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

... continues on next page ...

...continued from previous page ...
<p>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.</p>
<p><b>Impact</b></p> <p>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.</p> <p>Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>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.</p>
<p><b>Affected Software/OS</b></p> <p>All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.</p>
<p><b>Vulnerability Insight</b></p> <p>The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:</p> <ul style="list-style-type: none"> <li>- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)</li> <li>- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)</li> </ul>
<p><b>Vulnerability Detection Method</b></p> <p>Check the used TLS protocols of the services provided by this system.</p> <p>Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection</p> <p>OID:1.3.6.1.4.1.25623.1.0.117274</p> <p>Version used: 2024-09-27T05:05:23Z</p>
<p><b>Product Detection Result</b></p> <p>Product: cpe:/a:ietf:transport_layer_security:1.0</p> <p>Method: SSL/TLS: Version Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.105782)</p>
<p><b>References</b></p> <p>cve: CVE-2011-3389</p> <p>cve: CVE-2015-0204</p> <p>url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a></p> <p>url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a></p> <p>url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a></p> <p>url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a></p> <p>url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a></p>
... continues on next page ...

...continued from previous page ...

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

dfn-cert: DFN-CERT-2015-0374

dfn-cert: DFN-CERT-2015-0305

... continues on next page ...



...continued from previous page ...

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  
dfn-cert: DFN-CERT-2011-1844  
dfn-cert: DFN-CERT-2011-1826

...continues on next page ...

...continued from previous page ...

```
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
```

[\[ return to 192.168.68.56 \]](#)**2.12.6 Low general/icmp**

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**

The remote host responded to an ICMP timestamp request.

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

The following response / ICMP packet has been received:

- ICMP Type: 14
- ICMP Code: 0

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

... continues on next page ...

...continued from previous page ...
<p>Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.</p> <p>Details: ICMP Timestamp Reply Information Disclosure</p> <p>OID:1.3.6.1.4.1.25623.1.0.103190</p> <p>Version used: 2025-01-21T05:37:33Z</p>
<p><b>References</b></p> <p>cve: CVE-1999-0524</p> <p>url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a></p> <p>url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a></p> <p>cert-bund: CB-K15/1514</p> <p>cert-bund: CB-K14/0632</p> <p>dfn-cert: DFN-CERT-2014-0658</p>

[ [return to 192.168.68.56](#) ]

### 2.12.7 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<p><b>Summary</b></p> <p>The remote host implements TCP timestamps and therefore allows to compute the uptime.</p>
<p><b>Quality of Detection (QoD):</b> 80%</p>
<p><b>Vulnerability Detection Result</b></p> <p>It was detected that the host implements RFC1323/RFC7323.</p> <p>The following timestamps were retrieved with a delay of 1 seconds in-between:</p> <p>Packet 1: 19546011</p> <p>Packet 2: 19546724</p>
<p><b>Impact</b></p> <p>A side effect of this feature is that the uptime of the remote host can sometimes be computed.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.</p> <p>To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'</p> <p>Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.</p>
... continues on next page ...

...continued from previous page ...
See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a> url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a>

[ [return to 192.168.68.56](#) ]

2.13 192.168.68.58

Host scan start Mon Mar 3 15:59:07 2025 UTC  
Host scan end Mon Mar 3 16:38:48 2025 UTC

Service (Port)	Threat Level
<a href="#">8443/tcp</a>	Medium
<a href="#">9000/tcp</a>	Medium
<a href="#">10001/tcp</a>	Medium
<a href="#">general/tcp</a>	Low
<a href="#">general/icmp</a>	Low

2.13.1 Medium 8443/tcp

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
<b>Summary</b>
... continues on next page ...

...continued from previous page ...
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following certificates are part of the certificate chain but using insecure ↪signature algorithms: Subject: CN=AYF8GK FA8FCA80AD02,C=US,OU=Cast,ST=California,O=Google ↪ Inc,L=Mountain View Signature Algorithm: sha1WithRSAEncryption
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Vulnerability Insight</b> 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
<b>Vulnerability Detection Method</b> 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
<b>References</b> url: <a href="https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/">https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/</a>

## 2.13.2 Medium 9000/tcp

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
<p><b>Summary</b></p> <p>The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.</p>
<p><b>Quality of Detection (QoD):</b> 80%</p>
<p><b>Vulnerability Detection Result</b></p> <p>The following certificates are part of the certificate chain but using insecure ↪signature algorithms:</p> <p>Subject: CN=AYF8GK FA8FCA80AD02,C=US,OU=Cast,ST=California,O=Google  ↪ Inc,L=Mountain View</p> <p>Signature Algorithm: sha1WithRSAEncryption</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>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.</p>
<p><b>Vulnerability Insight</b></p> <p>The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:</p> <ul style="list-style-type: none"> <li>- Secure Hash Algorithm 1 (SHA-1)</li> <li>- Message Digest 5 (MD5)</li> <li>- Message Digest 4 (MD4)</li> <li>- Message Digest 2 (MD2)</li> </ul> <p>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.</p> <p>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:</p> <p>Fingerprint1  or  fingerprint1, Fingerprint2</p>
<p><b>Vulnerability Detection Method</b></p> <p>Check which hashing algorithm was used to sign the remote SSL/TLS certificate.</p> <p>Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm</p> <p>OID:1.3.6.1.4.1.25623.1.0.105880</p>
... continues on next page ...

...continued from previous page ...
Version used: 2021-10-15T11:13:32Z
<b>References</b> url: <a href="https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/">https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/</a>

[ [return to 192.168.68.58](#) ]

### 2.13.3 Medium 10001/tcp

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
<b>Summary</b> The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: CN=AYF8GK FA8FCA80AD02,C=US,OU=Cast,ST=California,O=Google Inc,L=Mountain View Signature Algorithm: sha1WithRSAEncryption
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Vulnerability Insight</b> 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.
... continues on next page ...

...continued from previous page ...
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
<b>Vulnerability Detection Method</b> 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
<b>References</b> url: <a href="https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/">https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/</a>

[ [return to 192.168.68.58](#) ]

#### 2.13.4 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 2225203 Packet 2: 2225356
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b> <b>Solution type:</b> Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
... continues on next page ...



...continued from previous page ...
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a> url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a>

[ [return to 192.168.68.58](#) ]

### 2.13.5 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: - ICMP Type: 14 - ICMP Code: 0
<b>Impact</b>
... continues on next page ...

...continued from previous page ...

This information could theoretically be used to exploit weak time-based random number generators in other services.

**Solution:**

**Solution type:** Mitigation

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: ICMP Timestamp Reply Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: 2025-01-21T05:37:33Z

**References**

cve: CVE-1999-0524

url: <https://datatracker.ietf.org/doc/html/rfc792>

url: <https://datatracker.ietf.org/doc/html/rfc2780>

cert-bund: CB-K15/1514

cert-bund: CB-K14/0632

dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.68.58 \]](#)

**2.14 192.168.68.86**

Host scan start Mon Mar 3 15:59:01 2025 UTC

Host scan end Mon Mar 3 17:04:49 2025 UTC

Service (Port)	Threat Level
<a href="#">general/icmp</a>	Low
<a href="#">general/tcp</a>	Low

**2.14.1 Low general/icmp**

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: - ICMP Type: 14 - ICMP Code: 0
<b>Impact</b> This information could theoretically be used to exploit weak time-based random number generators in other services.
<b>Solution:</b> <b>Solution type:</b> Mitigation Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)
<b>Vulnerability Insight</b> The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.
<b>Vulnerability Detection Method</b> Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2025-01-21T05:37:33Z
<b>References</b> cve: CVE-1999-0524 url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a> cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.68.86 \]](#)

**2.14.2 Low general/tcp**

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 1056694786 Packet 2: 1056695677
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b> <b>Solution type:</b> Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> ... continues on next page ...

...continued from previous page ...

```
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[ [return to 192.168.68.86](#) ]

## 2.15 192.168.68.88

Host scan start Mon Mar 3 15:59:01 2025 UTC

Host scan end Mon Mar 3 16:38:09 2025 UTC

Service (Port)	Threat Level
<a href="#">general/tcp</a>	Low
<a href="#">general/icmp</a>	Low

### 2.15.1 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

#### Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Quality of Detection (QoD): 80%

#### Vulnerability Detection Result

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:

Packet 1: 3543957514

Packet 2: 3543960490

#### Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

#### Solution:

**Solution type:** Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp\_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

... continues on next page ...

...continued from previous page ...
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a> url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a>

[ [return to 192.168.68.88](#) ]

### 2.15.2 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: - ICMP Type: 14 - ICMP Code: 0
<b>Impact</b>
... continues on next page ...

...continued from previous page ...
This information could theoretically be used to exploit weak time-based random number generators in other services.
<b>Solution:</b> <b>Solution type:</b> Mitigation Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)
<b>Vulnerability Insight</b> The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.
<b>Vulnerability Detection Method</b> Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2025-01-21T05:37:33Z
<b>References</b> cve: CVE-1999-0524 url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a> cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658

[ [return to 192.168.68.88](#) ]

## 2.16 192.168.68.82

Host scan start Mon Mar 3 15:59:01 2025 UTC  
 Host scan end Mon Mar 3 16:35:46 2025 UTC

Service (Port)	Threat Level
<a href="#">general/icmp</a>	Low
<a href="#">general/tcp</a>	Low

### 2.16.1 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: - ICMP Type: 14 - ICMP Code: 0
<b>Impact</b> This information could theoretically be used to exploit weak time-based random number generators in other services.
<b>Solution:</b> <b>Solution type:</b> Mitigation Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)
<b>Vulnerability Insight</b> The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.
<b>Vulnerability Detection Method</b> Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2025-01-21T05:37:33Z
<b>References</b> cve: CVE-1999-0524 url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a> cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.68.82 \]](#)



**2.16.2 Low general/tcp**

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 2831529 Packet 2: 2831642
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b> <b>Solution type:</b> Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> ... continues on next page ...

...continued from previous page ...

```
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[ [return to 192.168.68.82](#) ]

## 2.17 192.168.68.81

Host scan start Mon Mar 3 15:59:01 2025 UTC

Host scan end Mon Mar 3 17:55:10 2025 UTC

Service (Port)	Threat Level
<a href="#">general/tcp</a>	Low
<a href="#">general/icmp</a>	Low

### 2.17.1 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

**Summary**

The remote host implements TCP timestamps and therefore allows to compute the uptime.

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

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:

Packet 1: 244732848

Packet 2: 244733369

**Impact**

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

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

To disable TCP timestamps on linux add the line 'net.ipv4.tcp\_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

... continues on next page ...

...continued from previous page ...
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a> url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a>

[\[ return to 192.168.68.81 \]](#)

### 2.17.2 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: - ICMP Type: 14 - ICMP Code: 0
<b>Impact</b>
... continues on next page ...

...continued from previous page ...
This information could theoretically be used to exploit weak time-based random number generators in other services.
<b>Solution:</b> <b>Solution type:</b> Mitigation Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)
<b>Vulnerability Insight</b> The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.
<b>Vulnerability Detection Method</b> Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2025-01-21T05:37:33Z
<b>References</b> cve: CVE-1999-0524 url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a> cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658

[ [return to 192.168.68.81](#) ]

## 2.18 192.168.68.102

Host scan start Mon Mar 3 15:59:07 2025 UTC  
 Host scan end Mon Mar 3 17:54:29 2025 UTC

Service (Port)	Threat Level
<a href="#">general/tcp</a>	Low
<a href="#">general/icmp</a>	Low

### 2.18.1 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 244741074 Packet 2: 244741541
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b> <b>Solution type:</b> Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d</a> ... continues on next page ...

...continued from previous page ...

↩️ownload/details.aspx?id=9152

url: https://www.fortiguard.com/psirt/FG-IR-16-090

[\[ return to 192.168.68.102 \]](#)**2.18.2 Low general/icmp**

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**

The remote host responded to an ICMP timestamp request.

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

The following response / ICMP packet has been received:

- ICMP Type: 14
- ICMP Code: 0

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: ICMP Timestamp Reply Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: 2025-01-21T05:37:33Z

... continues on next page ...

...continued from previous page ...

**References**

cve: CVE-1999-0524

url: <https://datatracker.ietf.org/doc/html/rfc792>url: <https://datatracker.ietf.org/doc/html/rfc2780>

cert-bund: CB-K15/1514

cert-bund: CB-K14/0632

dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.68.102 \]](#)**2.19 192.168.68.80**

Host scan start Mon Mar 3 15:59:02 2025 UTC

Host scan end Mon Mar 3 17:56:41 2025 UTC

Service (Port)	Threat Level
<a href="#">general/icmp</a>	Low
<a href="#">general/tcp</a>	Low

**2.19.1 Low general/icmp**

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**

The remote host responded to an ICMP timestamp request.

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

The following response / ICMP packet has been received:

- ICMP Type: 14
- ICMP Code: 0

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely

... continues on next page ...

...continued from previous page ...
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)
<b>Vulnerability Insight</b> The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.
<b>Vulnerability Detection Method</b> Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2025-01-21T05:37:33Z
<b>References</b> cve: CVE-1999-0524 url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a> cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658

[ [return to 192.168.68.80](#) ]

### 2.19.2 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 97897189 Packet 2: 97897335
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
... continues on next page ...



...continued from previous page...

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

To disable TCP timestamps on linux add the line 'net.ipv4.tcp\_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

**Affected Software/OS**

TCP implementations that implement RFC1323/RFC7323.

**Vulnerability Insight**

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

**Vulnerability Detection Method**

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: TCP Timestamps Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: 2023-12-15T16:10:08Z

**References**

url: <https://datatracker.ietf.org/doc/html/rfc1323>

url: <https://datatracker.ietf.org/doc/html/rfc7323>

url: <https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152>

url: <https://www.fortiguard.com/psirt/FG-IR-16-090>

[\[ return to 192.168.68.80 \]](#)

**2.20 192.168.68.62**

Host scan start Mon Mar 3 16:30:46 2025 UTC

Host scan end Mon Mar 3 17:27:06 2025 UTC

Service (Port)	Threat Level
<a href="#">general/icmp</a>	Low
<a href="#">general/tcp</a>	Low

**2.20.1 Low general/icmp**

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: - ICMP Type: 14 - ICMP Code: 0
<b>Impact</b> This information could theoretically be used to exploit weak time-based random number generators in other services.
<b>Solution:</b> <b>Solution type:</b> Mitigation Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)
<b>Vulnerability Insight</b> The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.
<b>Vulnerability Detection Method</b> Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2025-01-21T05:37:33Z
<b>References</b> cve: CVE-1999-0524 url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a> cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.68.62 \]](#)

## 2.20.2 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 2556717 Packet 2: 2556856
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b> <b>Solution type:</b> Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> ... continues on next page ...

...continued from previous page ...

```
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[ [return to 192.168.68.62](#) ]

## 2.21 192.168.68.91

Host scan start Mon Mar 3 16:37:46 2025 UTC

Host scan end Mon Mar 3 17:17:22 2025 UTC

Service (Port)	Threat Level
<a href="#">general/tcp</a>	Low
<a href="#">general/icmp</a>	Low

### 2.21.1 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

**Summary**

The remote host implements TCP timestamps and therefore allows to compute the uptime.

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

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:

Packet 1: 1895991492

Packet 2: 1895991984

**Impact**

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

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

To disable TCP timestamps on linux add the line 'net.ipv4.tcp\_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'  
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

... continues on next page ...

...continued from previous page ...
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a> url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a>

[ [return to 192.168.68.91](#) ]

### 2.21.2 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: - ICMP Type: 14 - ICMP Code: 0
<b>Impact</b>
... continues on next page ...

...continued from previous page ...
This information could theoretically be used to exploit weak time-based random number generators in other services.
<b>Solution:</b> <b>Solution type:</b> Mitigation Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)
<b>Vulnerability Insight</b> The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.
<b>Vulnerability Detection Method</b> Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2025-01-21T05:37:33Z
<b>References</b> cve: CVE-1999-0524 url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a> cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.68.91 \]](#)

## 2.22 192.168.68.54

Host scan start Mon Mar 3 16:35:47 2025 UTC  
 Host scan end Mon Mar 3 17:24:24 2025 UTC

Service (Port)	Threat Level
<a href="#">general/tcp</a>	Low
<a href="#">general/icmp</a>	Low

### 2.22.1 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 808520387 Packet 2: 808521002
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b> <b>Solution type:</b> Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d</a> ... continues on next page ...

...continued from previous page ...

↩️ownload/details.aspx?id=9152

url: https://www.fortiguard.com/psirt/FG-IR-16-090

[\[ return to 192.168.68.54 \]](#)**2.22.2 Low general/icmp**

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**

The remote host responded to an ICMP timestamp request.

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

The following response / ICMP packet has been received:

- ICMP Type: 14
- ICMP Code: 0

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: ICMP Timestamp Reply Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: 2025-01-21T05:37:33Z

... continues on next page ...



...continued from previous page ...	
<b>References</b> cve: CVE-1999-0524 url: https://datatracker.ietf.org/doc/html/rfc792 url: https://datatracker.ietf.org/doc/html/rfc2780 cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658	

[ [return to 192.168.68.54](#) ]

2.23 192.168.68.75

Host scan start Mon Mar 3 17:24:25 2025 UTC  
Host scan end Mon Mar 3 17:55:40 2025 UTC

Service (Port)	Threat Level
<a href="#">general/tcp</a>	Low
<a href="#">general/icmp</a>	Low

2.23.1 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 256980594 Packet 2: 256980717
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b> <b>Solution type:</b> Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
... continues on next page ...

...continued from previous page ...
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a> url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a>

[ [return to 192.168.68.75](#) ]

2.23.2 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: - ICMP Type: 14 - ICMP Code: 0
... continues on next page ...

...continued from previous page ...

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

**Solution:**

**Solution type:** Mitigation

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: ICMP Timestamp Reply Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: 2025-01-21T05:37:33Z

**References**

cve: CVE-1999-0524

url: <https://datatracker.ietf.org/doc/html/rfc792>

url: <https://datatracker.ietf.org/doc/html/rfc2780>

cert-bund: CB-K15/1514

cert-bund: CB-K14/0632

dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.68.75 \]](#)

**2.24 192.168.68.100**

Host scan start Mon Mar 3 16:31:54 2025 UTC

Host scan end Mon Mar 3 17:54:16 2025 UTC

Service (Port)	Threat Level
<a href="#">general/tcp</a>	Low
<a href="#">general/icmp</a>	Low

**2.24.1 Low general/tcp**

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 3486764017 Packet 2: 3486765110
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b> <b>Solution type:</b> Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d</a> ... continues on next page ...

...continued from previous page ...

↩download/details.aspx?id=9152

url: <https://www.fortiguard.com/psirt/FG-IR-16-090>[\[ return to 192.168.68.100 \]](#)**2.24.2 Low general/icmp**

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**

The remote host responded to an ICMP timestamp request.

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

The following response / ICMP packet has been received:

- ICMP Type: 14
- ICMP Code: 0

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: ICMP Timestamp Reply Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: 2025-01-21T05:37:33Z

... continues on next page ...

...continued from previous page ...

**References**

cve: CVE-1999-0524

url: <https://datatracker.ietf.org/doc/html/rfc792>url: <https://datatracker.ietf.org/doc/html/rfc2780>

cert-bund: CB-K15/1514

cert-bund: CB-K14/0632

dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.68.100 \]](#)**2.25 192.168.68.98**

Host scan start Mon Mar 3 16:38:12 2025 UTC

Host scan end Mon Mar 3 17:27:23 2025 UTC

Service (Port)	Threat Level
<a href="#">general/tcp</a>	Low
<a href="#">general/icmp</a>	Low

**2.25.1 Low general/tcp**

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

**Summary**

The remote host implements TCP timestamps and therefore allows to compute the uptime.

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

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:

Packet 1: 7084735

Packet 2: 7085081

**Impact**

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

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

To disable TCP timestamps on linux add the line 'net.ipv4.tcp\_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

... continues on next page ...

...continued from previous page ...
<p>Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.</p>
<p><b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.</p>
<p><b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.</p>
<p><b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z</p>
<p><b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a> url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a></p>

[ [return to 192.168.68.98](#) ]

### 2.25.2 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<p><b>Summary</b> The remote host responded to an ICMP timestamp request.</p>
<p><b>Quality of Detection (QoD):</b> 80%</p>
<p><b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: - ICMP Type: 14 - ICMP Code: 0</p>
... continues on next page ...

...continued from previous page ...

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

**Solution:**

**Solution type:** Mitigation

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: ICMP Timestamp Reply Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: 2025-01-21T05:37:33Z

**References**

cve: CVE-1999-0524

url: <https://datatracker.ietf.org/doc/html/rfc792>

url: <https://datatracker.ietf.org/doc/html/rfc2780>

cert-bund: CB-K15/1514

cert-bund: CB-K14/0632

dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.68.98 \]](#)

**2.26 192.168.68.70**

Host scan start Mon Mar 3 17:17:43 2025 UTC

Host scan end Mon Mar 3 18:00:55 2025 UTC

Service (Port)	Threat Level
<a href="#">general/tcp</a>	Low
<a href="#">general/icmp</a>	Low

**2.26.1 Low general/tcp**



Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD): 80%</b>
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 98353043 Packet 2: 98353157
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b> <b>Solution type:</b> Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d</a> ... continues on next page ...

...continued from previous page ...

↩️ownload/details.aspx?id=9152

url: https://www.fortiguard.com/psirt/FG-IR-16-090

[\[ return to 192.168.68.70 \]](#)**2.26.2 Low general/icmp**

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**

The remote host responded to an ICMP timestamp request.

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

The following response / ICMP packet has been received:

- ICMP Type: 14
- ICMP Code: 0

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: ICMP Timestamp Reply Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: 2025-01-21T05:37:33Z

... continues on next page ...

...continued from previous page ...

**References**

cve: CVE-1999-0524  
 url: <https://datatracker.ietf.org/doc/html/rfc792>  
 url: <https://datatracker.ietf.org/doc/html/rfc2780>  
 cert-bund: CB-K15/1514  
 cert-bund: CB-K14/0632  
 dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.68.70 \]](#)**2.27 192.168.68.60**

Host scan start Mon Mar 3 17:39:23 2025 UTC  
 Host scan end Mon Mar 3 18:00:19 2025 UTC

Service (Port)	Threat Level
<a href="#">general/icmp</a>	Low
<a href="#">general/tcp</a>	Low

**2.27.1 Low general/icmp**

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**

The remote host responded to an ICMP timestamp request.

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

The following response / ICMP packet has been received:

- ICMP Type: 14
- ICMP Code: 0

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely

... continues on next page ...

...continued from previous page ...
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)
<b>Vulnerability Insight</b> The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.
<b>Vulnerability Detection Method</b> Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2025-01-21T05:37:33Z
<b>References</b> cve: CVE-1999-0524 url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a> cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658

[ [return to 192.168.68.60](#) ]

### 2.27.2 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 257482017 Packet 2: 257482187
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
... continues on next page ...

...continued from previous page...

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

To disable TCP timestamps on linux add the line 'net.ipv4.tcp\_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

**Affected Software/OS**

TCP implementations that implement RFC1323/RFC7323.

**Vulnerability Insight**

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

**Vulnerability Detection Method**

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: TCP Timestamps Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: 2023-12-15T16:10:08Z

**References**

url: <https://datatracker.ietf.org/doc/html/rfc1323>

url: <https://datatracker.ietf.org/doc/html/rfc7323>

url: <https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152>

url: <https://www.fortiguard.com/psirt/FG-IR-16-090>

[\[ return to 192.168.68.60 \]](#)

**2.28 192.168.68.84**

Host scan start Mon Mar 3 15:59:01 2025 UTC

Host scan end Mon Mar 3 17:38:46 2025 UTC

Service (Port)	Threat Level
<a href="#">general/icmp</a>	Low
<a href="#">general/tcp</a>	Low

**2.28.1 Low general/icmp**

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: - ICMP Type: 14 - ICMP Code: 0
<b>Impact</b> This information could theoretically be used to exploit weak time-based random number generators in other services.
<b>Solution:</b> <b>Solution type:</b> Mitigation Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)
<b>Vulnerability Insight</b> The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.
<b>Vulnerability Detection Method</b> Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2025-01-21T05:37:33Z
<b>References</b> cve: CVE-1999-0524 url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a> cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.68.84 \]](#)

**2.28.2 Low general/tcp**

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 330544696 Packet 2: 330545780
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b> <b>Solution type:</b> Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> ... continues on next page ...

...continued from previous page ...
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090

[ [return to 192.168.68.84](#) ]

2.29 192.168.68.72

Host scan start Mon Mar 3 17:39:04 2025 UTC  
Host scan end Mon Mar 3 17:59:22 2025 UTC

Service (Port)	Threat Level
<a href="#">general/tcp</a>	Low

2.29.1 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 309998354 Packet 2: 3659291033
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution:</b> <b>Solution type:</b> Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
... continues on next page ...



...continued from previous page ...
See the references for more information.
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a> url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a>

[ [return to 192.168.68.72](#) ]

## 2.30 192.168.68.97

Host scan start Mon Mar 3 15:59:04 2025 UTC  
Host scan end Mon Mar 3 17:56:35 2025 UTC

Service (Port)	Threat Level
<a href="#">general/icmp</a>	Low

### 2.30.1 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
... continues on next page ...

...continued from previous page ...

**Vulnerability Detection Result**

The following response / ICMP packet has been received:

- ICMP Type: 14
- ICMP Code: 0

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

**Solution:**

**Solution type:** Mitigation

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: ICMP Timestamp Reply Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: 2025-01-21T05:37:33Z

**References**

cve: CVE-1999-0524

url: <https://datatracker.ietf.org/doc/html/rfc792>

url: <https://datatracker.ietf.org/doc/html/rfc2780>

cert-bund: CB-K15/1514

cert-bund: CB-K14/0632

dfn-cert: DFN-CERT-2014-0658

[\[ return to 192.168.68.97 \]](#)