

Scan Report

January 17, 2023

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Immediate scan of IP 172.16.1.8 windows2012r2”. The scan started at Mon Jan 16 11:56:16 2023 UTC and ended at Mon Jan 16 12:14:17 2023 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1	Result Overview	2
2	Results per Host	2
2.1	172.16.1.8	2
2.1.1	High 443/tcp	2
2.1.2	High 80/tcp	7
2.1.3	High 445/tcp	8
2.1.4	Medium 443/tcp	10
2.1.5	Medium 135/tcp	22
2.1.6	Medium 3389/tcp	26
2.1.7	Low 443/tcp	34
2.1.8	Low general/tcp	37

1 Result Overview

Host	High	Medium	Low	Log	False Positive
172.16.1.8	4	11	2	0	0
Total: 1	4	11	2	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 17 results selected by the filtering described above. Before filtering there were 77 results.

2 Results per Host

2.1 172.16.1.8

Host scan start Mon Jan 16 11:56:43 2023 UTC

Host scan end Mon Jan 16 12:14:12 2023 UTC

Service (Port)	Threat Level
443/tcp	High
80/tcp	High
445/tcp	High
443/tcp	Medium
135/tcp	Medium
3389/tcp	Medium
443/tcp	Low
general/tcp	Low

2.1.1 High 443/tcp

High (CVSS: 10.0)

NVT: MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)

Product detection result

... continues on next page ...

...continued from previous page ...
<p>cpe:/a:microsoft:internet_information_services:8.5</p> <p>Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID: ↪ 1.3.6.1.4.1.25623.1.0.900710)</p>
<p>Summary</p> <p>This host is missing an important security update according to Microsoft Bulletin MS15-034.</p>
<p>Vulnerability Detection Result</p> <p>Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p>Impact</p> <p>Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.</p>
<p>Solution:</p> <p>Solution type: VendorFix</p> <p>The vendor has released updates. Please see the references for more information.</p>
<p>Affected Software/OS</p> <ul style="list-style-type: none"> - Microsoft Windows 8 x32/x64 - Microsoft Windows 8.1 x32/x64 - Microsoft Windows Server 2012 - Microsoft Windows Server 2012 R2 - Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior - Microsoft Windows 7 x32/x64 Service Pack 1 and prior
<p>Vulnerability Insight</p> <p>Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.</p>
<p>Vulnerability Detection Method</p> <p>Send a special crafted HTTP GET request and check the response</p> <p>Details: MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.105257</p> <p>Version used: 2022-12-05T10:11:03Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:microsoft:internet_information_services:8.5</p> <p>Method: Microsoft Internet Information Services (IIS) Detection (HTTP)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.900710)</p>
<p>References</p> <p>cve: CVE-2015-1635</p> <p>cisa: Known Exploited Vulnerability (KEV) catalog</p>
...continues on next page ...

...continued from previous page...

url: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
url: <https://support.microsoft.com/kb/3042553>
url: <https://technet.microsoft.com/library/security/MS15-034>
url: <http://pastebin.com/ypURDPc4>
cert-bund: CB-K15/0527
dfn-cert: DFN-CERT-2015-0545

High (CVSS: 7.5)

NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary

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

Vulnerability Detection Result

'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'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)

Solution:

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.

Please see the references for more resources supporting you with this task.

Affected Software/OS

Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight

These rules are applied for the evaluation of the vulnerable cipher suites:

- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method

Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

OID:1.3.6.1.4.1.25623.1.0.108031

Version used: 2022-08-01T10:11:45Z

References

cve: CVE-2016-2183

cve: CVE-2016-6329

cve: CVE-2020-12872

... continues on next page ...

...continued from previous page ...

```
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
```

... continues on next page ...

...continued from previous page ...

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-2021-1618
 dfn-cert: DFN-CERT-2021-0775
 dfn-cert: DFN-CERT-2021-0770
 dfn-cert: DFN-CERT-2021-0274
 dfn-cert: DFN-CERT-2020-2141
 dfn-cert: DFN-CERT-2020-0368
 dfn-cert: DFN-CERT-2019-1455
 dfn-cert: DFN-CERT-2019-0068
 dfn-cert: DFN-CERT-2018-1296
 dfn-cert: DFN-CERT-2018-0323
 dfn-cert: DFN-CERT-2017-2070
 dfn-cert: DFN-CERT-2017-1954
 dfn-cert: DFN-CERT-2017-1885
 dfn-cert: DFN-CERT-2017-1831
 dfn-cert: DFN-CERT-2017-1821
 dfn-cert: DFN-CERT-2017-1785
 dfn-cert: DFN-CERT-2017-1626
 dfn-cert: DFN-CERT-2017-1326
 dfn-cert: DFN-CERT-2017-1239
 dfn-cert: DFN-CERT-2017-1238
 dfn-cert: DFN-CERT-2017-1090
 dfn-cert: DFN-CERT-2017-1060
 dfn-cert: DFN-CERT-2017-0968
 dfn-cert: DFN-CERT-2017-0947
 dfn-cert: DFN-CERT-2017-0946
 dfn-cert: DFN-CERT-2017-0904
 dfn-cert: DFN-CERT-2017-0816
 dfn-cert: DFN-CERT-2017-0746
 dfn-cert: DFN-CERT-2017-0677
 dfn-cert: DFN-CERT-2017-0675
 dfn-cert: DFN-CERT-2017-0611
 dfn-cert: DFN-CERT-2017-0609
 dfn-cert: DFN-CERT-2017-0522
 dfn-cert: DFN-CERT-2017-0519
 dfn-cert: DFN-CERT-2017-0482
 dfn-cert: DFN-CERT-2017-0351
 dfn-cert: DFN-CERT-2017-0090
 dfn-cert: DFN-CERT-2017-0089
 dfn-cert: DFN-CERT-2017-0088
 dfn-cert: DFN-CERT-2017-0086
 dfn-cert: DFN-CERT-2016-1943

...continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[\[return to 172.16.1.8 \]](#)

2.1.2 High 80/tcp

High (CVSS: 10.0)
 NVT: MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)

Product detection result

cpe:/a:microsoft:internet_information_services:8.5

Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID:
 ↪ 1.3.6.1.4.1.25623.1.0.900710)

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-034.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior

... continues on next page ...

...continued from previous page ...
Vulnerability Insight Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.
Vulnerability Detection Method Send a special crafted HTTP GET request and check the response Details: MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check) OID:1.3.6.1.4.1.25623.1.0.105257 Version used: 2022-12-05T10:11:03Z
Product Detection Result Product: cpe:/a:microsoft:internet_information_services:8.5 Method: Microsoft Internet Information Services (IIS) Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.900710)
References cve: CVE-2015-1635 cisa: Known Exploited Vulnerability (KEV) catalog url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog url: https://support.microsoft.com/kb/3042553 url: https://technet.microsoft.com/library/security/MS15-034 url: http://pastebin.com/ypURDPc4 cert-bund: CB-K15/0527 dfn-cert: DFN-CERT-2015-0545

[\[return to 172.16.1.8 \]](#)

2.1.3 High 445/tcp

High (CVSS: 8.1) NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)
Summary This host is missing a critical security update according to Microsoft Bulletin MS17-010.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.
Solution: Solution type: VendorFix
... continues on next page ...

...continued from previous page ...
The vendor has released updates. Please see the references for more information.
Affected Software/OS <ul style="list-style-type: none"> - Microsoft Windows 10 x32/x64 - Microsoft Windows Server 2012 - Microsoft Windows Server 2016 - Microsoft Windows 8.1 x32/x64 - Microsoft Windows Server 2012 R2 - Microsoft Windows 7 x32/x64 Service Pack 1 - Microsoft Windows Vista x32/x64 Service Pack 2 - Microsoft Windows Server 2008 R2 x64 Service Pack 1 - Microsoft Windows Server 2008 x32/x64 Service Pack 2
Vulnerability Insight <p>Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.</p>
Vulnerability Detection Method <p>Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.</p> <p>Details: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) OID:1.3.6.1.4.1.25623.1.0.810676 Version used: 2022-08-09T10:11:17Z</p>
References <p>cve: CVE-2017-0143 cve: CVE-2017-0144 cve: CVE-2017-0145 cve: CVE-2017-0146 cve: CVE-2017-0147 cve: CVE-2017-0148 cisa: Known Exploited Vulnerability (KEV) catalog url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog url: https://support.microsoft.com/en-us/kb/4013078 url: http://www.securityfocus.com/bid/96703 url: http://www.securityfocus.com/bid/96704 url: http://www.securityfocus.com/bid/96705 url: http://www.securityfocus.com/bid/96707 url: http://www.securityfocus.com/bid/96709 url: http://www.securityfocus.com/bid/96706 url: https://technet.microsoft.com/library/security/MS17-010 url: https://github.com/rapid7/metasploit-framework/pull/8167/files cert-bund: CB-K17/0435 dfn-cert: DFN-CERT-2017-0448</p>

[[return to 172.16.1.8](#)]

2.1.4 Medium 443/tcp

Medium (CVSS: 5.9) NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
Summary It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.
Vulnerability Detection Result In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020.67) VT.
Impact An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.
Solution: Solution type: Mitigation It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
Affected Software/OS All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.
Vulnerability Insight The SSLv2 and SSLv3 protocols contain known cryptographic flaws like: - CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE) - CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)
Vulnerability Detection Method Check the used SSL protocols of the services provided by this system. Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.111012 Version used: 2021-10-15T12:51:02Z
References cve: CVE-2016-0800 cve: CVE-2014-3566 url: https://ssl-config.mozilla.org/ url: https://bettercrypto.org/ url: https://drownattack.com/ ... continues on next page ...

...continued from previous page...	
url:	https://www.imperialviolet.org/2014/10/14/poodle.html
url:	https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
	\hookrightarrow -report-2014
cert-bund:	CB-K18/0094
cert-bund:	CB-K17/1198
cert-bund:	CB-K17/1196
cert-bund:	CB-K16/1828
cert-bund:	CB-K16/1438
cert-bund:	CB-K16/1384
cert-bund:	CB-K16/1141
cert-bund:	CB-K16/1107
cert-bund:	CB-K16/1102
cert-bund:	CB-K16/0792
cert-bund:	CB-K16/0599
cert-bund:	CB-K16/0597
cert-bund:	CB-K16/0459
cert-bund:	CB-K16/0456
cert-bund:	CB-K16/0433
cert-bund:	CB-K16/0424
cert-bund:	CB-K16/0415
cert-bund:	CB-K16/0413
cert-bund:	CB-K16/0374
cert-bund:	CB-K16/0367
cert-bund:	CB-K16/0331
cert-bund:	CB-K16/0329
cert-bund:	CB-K16/0328
cert-bund:	CB-K16/0156
cert-bund:	CB-K15/1514
cert-bund:	CB-K15/1358
cert-bund:	CB-K15/1021
cert-bund:	CB-K15/0972
cert-bund:	CB-K15/0637
cert-bund:	CB-K15/0590
cert-bund:	CB-K15/0525
cert-bund:	CB-K15/0393
cert-bund:	CB-K15/0384
cert-bund:	CB-K15/0287
cert-bund:	CB-K15/0252
cert-bund:	CB-K15/0246
cert-bund:	CB-K15/0237
cert-bund:	CB-K15/0118
cert-bund:	CB-K15/0110
cert-bund:	CB-K15/0108
cert-bund:	CB-K15/0080
cert-bund:	CB-K15/0078
cert-bund:	CB-K15/0077
cert-bund:	CB-K15/0075
... continues on next page ...	

...continued from previous page ...

cert-bund: CB-K14/1617
 cert-bund: CB-K14/1581
 cert-bund: CB-K14/1537
 cert-bund: CB-K14/1479
 cert-bund: CB-K14/1458
 cert-bund: CB-K14/1342
 cert-bund: CB-K14/1314
 cert-bund: CB-K14/1313
 cert-bund: CB-K14/1311
 cert-bund: CB-K14/1304
 cert-bund: CB-K14/1296
 dfn-cert: DFN-CERT-2018-0096
 dfn-cert: DFN-CERT-2017-1238
 dfn-cert: DFN-CERT-2017-1236
 dfn-cert: DFN-CERT-2016-1929
 dfn-cert: DFN-CERT-2016-1527
 dfn-cert: DFN-CERT-2016-1468
 dfn-cert: DFN-CERT-2016-1216
 dfn-cert: DFN-CERT-2016-1174
 dfn-cert: DFN-CERT-2016-1168
 dfn-cert: DFN-CERT-2016-0884
 dfn-cert: DFN-CERT-2016-0841
 dfn-cert: DFN-CERT-2016-0644
 dfn-cert: DFN-CERT-2016-0642
 dfn-cert: DFN-CERT-2016-0496
 dfn-cert: DFN-CERT-2016-0495
 dfn-cert: DFN-CERT-2016-0465
 dfn-cert: DFN-CERT-2016-0459
 dfn-cert: DFN-CERT-2016-0453
 dfn-cert: DFN-CERT-2016-0451
 dfn-cert: DFN-CERT-2016-0415
 dfn-cert: DFN-CERT-2016-0403
 dfn-cert: DFN-CERT-2016-0388
 dfn-cert: DFN-CERT-2016-0360
 dfn-cert: DFN-CERT-2016-0359
 dfn-cert: DFN-CERT-2016-0357
 dfn-cert: DFN-CERT-2016-0171
 dfn-cert: DFN-CERT-2015-1431
 dfn-cert: DFN-CERT-2015-1075
 dfn-cert: DFN-CERT-2015-1026
 dfn-cert: DFN-CERT-2015-0664
 dfn-cert: DFN-CERT-2015-0548
 dfn-cert: DFN-CERT-2015-0404
 dfn-cert: DFN-CERT-2015-0396
 dfn-cert: DFN-CERT-2015-0259
 dfn-cert: DFN-CERT-2015-0254
 dfn-cert: DFN-CERT-2015-0245

...continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

Medium (CVSS: 5.0)

NVT: SSL/TLS: Report Weak Cipher Suites

Summary

This routine reports all Weak SSL/TLS cipher suites accepted by a service.

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

Vulnerability Detection Result

'Weak' cipher suites accepted by this service via the SSLv3 protocol:

TLS_RSA_WITH_RC4_128_MD5

TLS_RSA_WITH_RC4_128_SHA

'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_RSA_WITH_RC4_128_MD5

TLS_RSA_WITH_RC4_128_SHA

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

TLS_RSA_WITH_RC4_128_MD5

TLS_RSA_WITH_RC4_128_SHA

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

TLS_RSA_WITH_RC4_128_MD5

TLS_RSA_WITH_RC4_128_SHA

Solution:

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

Please see the references for more resources supporting you with this task.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength:

... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808) - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000) - 1024 bit RSA authentication is considered to be insecure and therefore as weak - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong
Vulnerability Detection Method Details: SSL/TLS: Report Weak Cipher Suites OID:1.3.6.1.4.1.25623.1.0.103440 Version used: 2021-12-01T13:10:37Z
References cve: CVE-2013-2566 cve: CVE-2015-2808 cve: CVE-2015-4000 url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1↪465_update_6.html url: https://bettercrypto.org/ url: https://mozilla.github.io/server-side-tls/ssl-config-generator/ cert-bund: CB-K21/0067 cert-bund: CB-K19/0812 cert-bund: CB-K17/1750 cert-bund: CB-K16/1593 cert-bund: CB-K16/1552 cert-bund: CB-K16/1102 cert-bund: CB-K16/0617 cert-bund: CB-K16/0599 cert-bund: CB-K16/0168 cert-bund: CB-K16/0121 cert-bund: CB-K16/0090 cert-bund: CB-K16/0030 cert-bund: CB-K15/1751 cert-bund: CB-K15/1591 cert-bund: CB-K15/1550 cert-bund: CB-K15/1517 cert-bund: CB-K15/1514 cert-bund: CB-K15/1464 cert-bund: CB-K15/1442 cert-bund: CB-K15/1334 cert-bund: CB-K15/1269 cert-bund: CB-K15/1136 cert-bund: CB-K15/1090 cert-bund: CB-K15/1059 cert-bund: CB-K15/1022 cert-bund: CB-K15/1015 cert-bund: CB-K15/0986
...continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038

...continues on next page ...

...continued from previous page ...

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

Medium (CVSS: 5.0)

NVT: SSL/TLS: Certificate Expired

Summary

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

Vulnerability Detection Result

The certificate of the remote service expired on 2020-01-07 07:23:34.

Certificate details:

```
fingerprint (SHA-1)      | F7827AF48BE62541331714258B7AE14CA0B9CAE9
fingerprint (SHA-256)    | F2669F9630635FCAC65419CA778B7063CB7AAFF564CB2F
↪E0842AA482D889EE3D
issued by                | CN=uacsrvt1.mycosendai.local
public key algorithm      | RSA
public key size (bits)    | 2048
serial                   | 1677A3846A7FCAAF4B88FAAFBE01866D
signature algorithm       | sha1WithRSAEncryption
subject                   | CN=uacsrvt1.mycosendai.local
subject alternative names (SAN) | None
valid from                | 2019-07-08 07:23:34 UTC
valid until               | 2020-01-07 07:23:34 UTC
```

Solution:

Solution type: Mitigation

Replace the SSL/TLS certificate by a new one.

...continues on next page ...

...continued from previous page ...

Vulnerability Insight

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

Vulnerability Detection Method

Details: SSL/TLS: Certificate Expired

OID:1.3.6.1.4.1.25623.1.0.103955

Version used: 2021-11-22T15:32:39Z

Medium (CVSS: 4.3)

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

Summary

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

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:

- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method

... continues on next page ...

...continued from previous page ...
<p>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: 2021-07-19T08:11:48Z</p>
<p>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: 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</p>
...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170

...continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)

NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result

Server Temporary Key Size: 1024 bits

Impact

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution:

Solution type: Workaround

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).

For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Checks the DHE temporary public key size. Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability. ↪... OID:1.3.6.1.4.1.25623.1.0.106223 Version used: 2021-02-12T06:42:15Z
References url: https://weakdh.org/ url: https://weakdh.org/sysadmin.html

Medium (CVSS: 4.0) NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
Summary The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.
Vulnerability Detection Result The following certificates are part of the certificate chain but using insecure ↪signature algorithms: Subject: CN=uacsrvt1.mycosendai.local Signature Algorithm: sha1WithRSAEncryption
Solution: Solution type: Mitigation Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.
Vulnerability Insight The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use: - Secure Hash Algorithm 1 (SHA-1) - Message Digest 5 (MD5) - Message Digest 4 (MD4) - Message Digest 2 (MD2) Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates. NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive: Fingerprint1 or ... continues on next page ...

...continued from previous page ...
fingerprint1, Fingerprint2
Vulnerability Detection Method Check which hashing algorithm was used to sign the remote SSL/TLS certificate. Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm OID:1.3.6.1.4.1.25623.1.0.105880 Version used: 2021-10-15T11:13:32Z
References url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

[[return to 172.16.1.8](#)]

2.1.5 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.
Vulnerability Detection Result Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol: Port: 49152/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:172.16.1.8[49152] Port: 49153/tcp UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:172.16.1.8[49153] Annotation: NRP server endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:172.16.1.8[49153] Annotation: DHCP Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:172.16.1.8[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1 Endpoint: ncacn_ip_tcp:172.16.1.8[49153] Annotation: Wcm Service UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:172.16.1.8[49153] Annotation: Event log TCPIP
... continues on next page ...

...continued from previous page...

Port: 49154/tcp

UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1

Endpoint: ncacn_ip_tcp:172.16.1.8[49154]

Annotation: IdSegSrv service

UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1

Endpoint: ncacn_ip_tcp:172.16.1.8[49154]

Annotation: Proxy Manager provider server endpoint

UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1

Endpoint: ncacn_ip_tcp:172.16.1.8[49154]

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

Endpoint: ncacn_ip_tcp:172.16.1.8[49154]

UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1

Endpoint: ncacn_ip_tcp:172.16.1.8[49154]

Annotation: IP Transition Configuration endpoint

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

Endpoint: ncacn_ip_tcp:172.16.1.8[49154]

UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1

Endpoint: ncacn_ip_tcp:172.16.1.8[49154]

Annotation: XactSrv service

UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1

Endpoint: ncacn_ip_tcp:172.16.1.8[49154]

Annotation: Proxy Manager client server endpoint

UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1

Endpoint: ncacn_ip_tcp:172.16.1.8[49154]

Annotation: Adh APIs

UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1

Endpoint: ncacn_ip_tcp:172.16.1.8[49154]

Annotation: Impl friendly name

Port: 49155/tcp

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

Endpoint: ncacn_ip_tcp:172.16.1.8[49155]

Annotation: RemoteAccessCheck

UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1

Endpoint: ncacn_ip_tcp:172.16.1.8[49155]

Named pipe : lsass

Win32 service or process : Netlogon

Description : Net Logon service

UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0

Endpoint: ncacn_ip_tcp:172.16.1.8[49155]

Named pipe : lsass

Win32 service or process : lsass.exe

Description : LSA access

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

Endpoint: ncacn_ip_tcp:172.16.1.8[49155]

Named pipe : lsass

Win32 service or process : lsass.exe

Description : SAM access

...continues on next page...

...continued from previous page...	
UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1	
Endpoint: ncacn_ip_tcp:172.16.1.8[49155]	
Annotation: Impl friendly name	
UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4	
Endpoint: ncacn_ip_tcp:172.16.1.8[49155]	
Annotation: MS NT Directory DRS Interface	
Port: 49157/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_http:172.16.1.8[49157]	
Annotation: RemoteAccessCheck	
UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1	
Endpoint: ncacn_http:172.16.1.8[49157]	
Named pipe : lsass	
Win32 service or process : Netlogon	
Description : Net Logon service	
UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0	
Endpoint: ncacn_http:172.16.1.8[49157]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : LSA access	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_http:172.16.1.8[49157]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4	
Endpoint: ncacn_http:172.16.1.8[49157]	
Annotation: MS NT Directory DRS Interface	
Port: 49158/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_ip_tcp:172.16.1.8[49158]	
Annotation: RemoteAccessCheck	
UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1	
Endpoint: ncacn_ip_tcp:172.16.1.8[49158]	
Named pipe : lsass	
Win32 service or process : Netlogon	
Description : Net Logon service	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:172.16.1.8[49158]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
Port: 49159/tcp	
UUID: 0b6edbf8-4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:172.16.1.8[49159]	
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1	
Endpoint: ncacn_ip_tcp:172.16.1.8[49159]	
...continues on next page...	

...continued from previous page...

Named pipe : spoolss
 Win32 service or process : spoolsv.exe
 Description : Spooler service
 UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
 Endpoint: ncacn_ip_tcp:172.16.1.8[49159]
 UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
 Endpoint: ncacn_ip_tcp:172.16.1.8[49159]
 UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
 Endpoint: ncacn_ip_tcp:172.16.1.8[49159]
 Port: 49164/tcp
 UUID: 32e36e84-4ba2-496c-ba85-fb450f325107, version 2
 Endpoint: ncacn_ip_tcp:172.16.1.8[49164]
 UUID: aa177641-fc9b-41bd-80ff-f964a701596f, version 1
 Endpoint: ncacn_ip_tcp:172.16.1.8[49164]
 Port: 49167/tcp
 UUID: 5b821720-f63b-11d0-aad2-00c04fc324db, version 1
 Endpoint: ncacn_ip_tcp:172.16.1.8[49167]
 UUID: 6bffd098-a112-3610-9833-46c3f874532d, version 1
 Endpoint: ncacn_ip_tcp:172.16.1.8[49167]
 Port: 49169/tcp
 UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
 Endpoint: ncacn_ip_tcp:172.16.1.8[49169]
 Port: 49173/tcp
 UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5
 Endpoint: ncacn_ip_tcp:172.16.1.8[49173]
 Named pipe : dnsserver
 Win32 service or process : dns.exe
 Description : DNS Server
 Port: 49175/tcp
 UUID: 89759fce-5a25-4086-8967-de12f39a60b5, version 1
 Endpoint: ncacn_ip_tcp:172.16.1.8[49175]
 UUID: 9b3195fe-d603-43d1-a0d5-9072d7cde122, version 1
 Endpoint: ncacn_ip_tcp:172.16.1.8[49175]
 Port: 49191/tcp
 UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1
 Endpoint: ncacn_ip_tcp:172.16.1.8[49191]
 Annotation: Frs2 Service
 Port: 5504/tcp
 UUID: ed96b012-c8ce-4f60-a682-35535b12ff75, version 2
 Endpoint: ncacn_ip_tcp:172.16.1.8[5504]
 Note: DCE/RPC or MSRPC services running on this host locally were identified. Re-
 porting this list is not enabled by default due to the possible large size of
 this list. See the script preferences to enable this reporting.

Impact

An attacker may use this fact to gain more knowledge about the remote host.

...continues on next page...

...continued from previous page ...

Solution:**Solution type:** Mitigation

Filter incoming traffic to this ports.

Vulnerability Detection Method

Details: DCE/RPC and MSRPC Services Enumeration Reporting

OID:1.3.6.1.4.1.25623.1.0.10736

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

[\[return to 172.16.1.8 \]](#)**2.1.6 Medium 3389/tcp**

Medium (CVSS: 5.0)

NVT: SSL/TLS: Report Weak Cipher Suites

Summary

This routine reports all Weak SSL/TLS cipher suites accepted by a service.

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

Vulnerability Detection Result

'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_RSA_WITH_RC4_128_MD5

TLS_RSA_WITH_RC4_128_SHA

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

TLS_RSA_WITH_RC4_128_MD5

TLS_RSA_WITH_RC4_128_SHA

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

TLS_RSA_WITH_RC4_128_MD5

TLS_RSA_WITH_RC4_128_SHA

Solution:**Solution type:** Mitigation

The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

Please see the references for more resources supporting you with this task.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength:

- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)

- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)

... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - 1024 bit RSA authentication is considered to be insecure and therefore as weak - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong
Vulnerability Detection Method Details: SSL/TLS: Report Weak Cipher Suites OID:1.3.6.1.4.1.25623.1.0.103440 Version used: 2021-12-01T13:10:37Z
References cve: CVE-2013-2566 cve: CVE-2015-2808 cve: CVE-2015-4000 url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1↪465_update_6.html url: https://bettercrypto.org/ url: https://mozilla.github.io/server-side-tls/ssl-config-generator/ cert-bund: CB-K21/0067 cert-bund: CB-K19/0812 cert-bund: CB-K17/1750 cert-bund: CB-K16/1593 cert-bund: CB-K16/1552 cert-bund: CB-K16/1102 cert-bund: CB-K16/0617 cert-bund: CB-K16/0599 cert-bund: CB-K16/0168 cert-bund: CB-K16/0121 cert-bund: CB-K16/0090 cert-bund: CB-K16/0030 cert-bund: CB-K15/1751 cert-bund: CB-K15/1591 cert-bund: CB-K15/1550 cert-bund: CB-K15/1517 cert-bund: CB-K15/1514 cert-bund: CB-K15/1464 cert-bund: CB-K15/1442 cert-bund: CB-K15/1334 cert-bund: CB-K15/1269 cert-bund: CB-K15/1136 cert-bund: CB-K15/1090 cert-bund: CB-K15/1059 cert-bund: CB-K15/1022 cert-bund: CB-K15/1015 cert-bund: CB-K15/0986 cert-bund: CB-K15/0964 cert-bund: CB-K15/0962 cert-bund: CB-K15/0932
...continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980

...continues on next page ...

...continued from previous page ...

```

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

```

Medium (CVSS: 4.3)

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

Summary

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

Vulnerability Detection Result

In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and ↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c ↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1 ↪.25623.1.0.802067) VT.

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:

Solution type: Mitigation

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

Affected Software/OS

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

Vulnerability Insight

... continues on next page ...

...continued from previous page ...
<p>The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:</p> <ul style="list-style-type: none"> - 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)
<p>Vulnerability Detection Method</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: 2021-07-19T08:11:48Z</p>
<p>References</p> <p>cve: CVE-2011-3389</p> <p>cve: CVE-2015-0204</p> <p>url: https://ssl-config.mozilla.org/</p> <p>url: https://bettercrypto.org/</p> <p>url: https://datatracker.ietf.org/doc/rfc8996/</p> <p>url: https://vnhacker.blogspot.com/2011/09/beast.html</p> <p>url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</p> <p>url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</p> <p>↔-report-2014</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> <p>cert-bund: CB-K14/0231</p> <p>cert-bund: CB-K13/0845</p> <p>cert-bund: CB-K13/0796</p> <p>cert-bund: CB-K13/0790</p> <p>dfn-cert: DFN-CERT-2020-0177</p> <p>dfn-cert: DFN-CERT-2020-0111</p>
...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

```

Medium (CVSS: 4.0)

NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary

The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

The following certificates are part of the certificate chain but using insecure ↔signature algorithms:

Subject: CN=uacsrvt1.mycosendai.local

Signature Algorithm: sha1WithRSAEncryption

Solution:

Solution type: Mitigation

Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

... continues on next page ...

...continued from previous page ...

Vulnerability Insight

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:

- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.

NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:

Fingerprint1

or

fingerprint1, Fingerprint2

Vulnerability Detection Method

Check which hashing algorithm was used to sign the remote SSL/TLS certificate.

Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

OID:1.3.6.1.4.1.25623.1.0.105880

Version used: 2021-10-15T11:13:32Z

References

url: <https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/>

Medium (CVSS: 4.0)

NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result

Server Temporary Key Size: 1024 bits

Impact

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution:

Solution type: Workaround

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).

For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

... continues on next page ...

...continued from previous page ...
<p>Vulnerability Insight</p> <p>The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.</p>
<p>Vulnerability Detection Method</p> <p>Checks the DHE temporary public key size.</p> <p>Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability. ↔...</p> <p>OID:1.3.6.1.4.1.25623.1.0.106223</p> <p>Version used: 2021-02-12T06:42:15Z</p>
<p>References</p> <p>url: https://weakdh.org/</p> <p>url: https://weakdh.org/sysadmin.html</p>

[\[return to 172.16.1.8 \]](#)

2.1.7 Low 443/tcp

<p>Low (CVSS: 3.4)</p> <p>NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)</p>
<p>Summary</p> <p>This host is prone to an information disclosure vulnerability.</p>
<p>Vulnerability Detection Result</p> <p>Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p>Impact</p> <p>Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.</p>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>Possible Mitigations are:</p> <ul style="list-style-type: none"> - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+
<p>Vulnerability Insight</p> <p>... continues on next page ...</p>

...continued from previous page ...
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code
Vulnerability Detection Method Evaluate previous collected information about this service. Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability . ↪.. OID:1.3.6.1.4.1.25623.1.0.802087 Version used: 2022-04-14T11:24:11Z
References cve: CVE-2014-3566 url: https://www.openssl.org/~bodo/ssl-poodle.pdf url: http://www.securityfocus.com/bid/70574 url: https://www.imperialviolet.org/2014/10/14/poodle.html url: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html url: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin-ssl-30.html ↪g-ssl-30.html cert-bund: CB-K17/1198 cert-bund: CB-K17/1196 cert-bund: CB-K16/1828 cert-bund: CB-K16/1438 cert-bund: CB-K16/1384 cert-bund: CB-K16/1102 cert-bund: CB-K16/0599 cert-bund: CB-K16/0156 cert-bund: CB-K15/1514 cert-bund: CB-K15/1358 cert-bund: CB-K15/1021 cert-bund: CB-K15/0972 cert-bund: CB-K15/0637 cert-bund: CB-K15/0590 cert-bund: CB-K15/0525 cert-bund: CB-K15/0393 cert-bund: CB-K15/0384 cert-bund: CB-K15/0287 cert-bund: CB-K15/0252 cert-bund: CB-K15/0246 cert-bund: CB-K15/0237 cert-bund: CB-K15/0118 cert-bund: CB-K15/0110 cert-bund: CB-K15/0108 cert-bund: CB-K15/0080 cert-bund: CB-K15/0078 cert-bund: CB-K15/0077 cert-bund: CB-K15/0075 cert-bund: CB-K14/1617
...continues on next page ...

...continued from previous page ...

```
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[\[return to 172.16.1.8 \]](#)

2.1.8 Low general/tcp

Low (CVSS: 2.6) NVT: TCP timestamps
Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.
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: 54419 Packet 2: 54523
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. Details: TCP timestamps OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2020-08-24T08:40:10Z
References url: http://www.ietf.org/rfc/rfc1323.txt url: http://www.ietf.org/rfc/rfc7323.txt url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

[\[return to 172.16.1.8 \]](#)

This file was automatically generated.