

Scan Report

May 6, 2024

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 “Compwire 192.168.0.0/24”. The scan started at Sun May 5 03:00:38 2024 UTC and ended at Sun May 5 15:19:27 2024 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
1.1	Host Authentications	4
2	Results per Host	4
2.1	192.168.0.200	4
2.1.1	High 80/tcp	4
2.1.2	Medium 3389/tcp	40
2.1.3	Medium 135/tcp	47
2.1.4	Medium 80/tcp	50
2.1.5	Low general/icmp	65
2.2	192.168.0.42	67
2.2.1	High 443/tcp	67
2.2.2	Medium 443/tcp	71
2.2.3	Medium 21/tcp	78
2.2.4	Medium 25/tcp	79
2.2.5	Low 22/tcp	85
2.2.6	Low general/icmp	86
2.3	192.168.0.6	87
2.3.1	Medium 3389/tcp	87
2.3.2	Medium 135/tcp	94
2.4	192.168.0.241	97
2.4.1	Medium 135/tcp	97

2.4.2	Medium 3389/tcp	100
2.4.3	Low general/icmp	107
2.5	192.168.0.252	108
2.5.1	Medium 443/tcp	108
2.5.2	Low general/icmp	114
2.6	192.168.0.125	116
2.6.1	Medium 443/tcp	116
2.6.2	Medium 135/tcp	123
2.6.3	Medium 3389/tcp	126
2.6.4	Medium 21/tcp	132
2.6.5	Medium 80/tcp	133
2.6.6	Low general/icmp	134
2.7	192.168.0.143	135
2.7.1	Medium 135/tcp	136
2.7.2	Medium 3389/tcp	138
2.7.3	Low general/icmp	144
2.8	192.168.0.202	146
2.8.1	Medium 3389/tcp	146
2.8.2	Medium 135/tcp	152
2.8.3	Low general/icmp	155
2.9	192.168.0.168	156
2.9.1	Medium 3389/tcp	156
2.9.2	Medium 135/tcp	163
2.9.3	Low general/icmp	166
2.10	192.168.0.250	167
2.10.1	Medium 135/tcp	167
2.10.2	Medium 3389/tcp	171
2.10.3	Low general/icmp	177
2.11	192.168.0.65	179
2.11.1	Medium 21/tcp	179
2.11.2	Medium 3389/tcp	180
2.11.3	Medium 135/tcp	186
2.11.4	Low general/icmp	189
2.12	192.168.0.3	190
2.12.1	Medium 3389/tcp	191
2.12.2	Medium 135/tcp	197
2.12.3	Low general/icmp	200
2.13	192.168.0.220	202
2.13.1	Medium 135/tcp	202
2.13.2	Medium 3389/tcp	205

2.13.3	Low general/icmp	212
2.14	192.168.0.254	213
2.14.1	Medium 443/tcp	213
2.15	192.168.0.15	221
2.15.1	Medium 25/tcp	221
2.15.2	Medium 22/tcp	229
2.15.3	Medium 443/tcp	230
2.15.4	Low 22/tcp	232
2.15.5	Low general/icmp	233
2.16	192.168.0.249	234
2.16.1	Medium 22/tcp	234
2.16.2	Low general/icmp	237
2.17	192.168.0.201	238
2.17.1	Medium 22/tcp	238
2.17.2	Medium 80/tcp	239
2.17.3	Low 22/tcp	240
2.17.4	Low general/icmp	241
2.18	192.168.0.2	242
2.18.1	Medium 443/tcp	242
2.18.2	Low general/icmp	245
2.18.3	Low 22/tcp	246
2.19	192.168.0.16	247
2.19.1	Medium 135/tcp	248
2.19.2	Low general/icmp	253
2.20	192.168.0.142	254
2.20.1	Medium 25/tcp	254
2.20.2	Low general/icmp	259
2.20.3	Low 22/tcp	260
2.21	192.168.0.5	261
2.21.1	Medium 25/tcp	262
2.21.2	Low 22/tcp	267
2.21.3	Low general/icmp	268
2.22	192.168.0.141	269
2.22.1	Medium 25/tcp	269
2.22.2	Low 22/tcp	275
2.22.3	Low general/icmp	276
2.23	192.168.0.9	277
2.23.1	Medium 135/tcp	277
2.23.2	Low general/icmp	282
2.24	192.168.0.209	284

2.24.1	Medium 443/tcp	284
2.24.2	Low general/icmp	285
2.24.3	Low 22/tcp	286
2.25	192.168.0.106	287
2.25.1	Medium 135/tcp	287
2.25.2	Low general/icmp	290
2.26	192.168.0.57	291
2.26.1	Medium 80/tcp	291
2.26.2	Medium 25/tcp	293
2.26.3	Low 22/tcp	298
2.26.4	Low general/icmp	299
2.27	192.168.0.28	300
2.27.1	Medium 25/tcp	301
2.27.2	Low 22/tcp	306
2.27.3	Low general/icmp	307
2.28	192.168.0.99	308
2.28.1	Medium 135/tcp	308
2.28.2	Low general/icmp	312
2.29	192.168.0.25	313
2.29.1	Medium 3389/tcp	313
2.29.2	Medium 135/tcp	316
2.29.3	Low general/icmp	318
2.30	192.168.0.104	319
2.30.1	Medium 25/tcp	320
2.30.2	Low 22/tcp	325
2.30.3	Low general/icmp	326
2.31	192.168.0.246	327
2.31.1	Medium 80/tcp	328
2.31.2	Low general/icmp	329
2.31.3	Low 22/tcp	330
2.32	192.168.0.130	331
2.32.1	Medium 80/tcp	331
2.32.2	Low 22/tcp	332
2.32.3	Low general/icmp	333
2.33	192.168.0.61	334
2.33.1	Medium 443/tcp	334
2.33.2	Low general/icmp	338
2.33.3	Low 22/tcp	339
2.34	192.168.0.97	340
2.34.1	Medium 443/tcp	340

2.35	192.168.0.245	343
2.35.1	Low general/icmp	343
2.35.2	Low 22/tcp	344
2.36	192.168.0.67	345
2.36.1	Low 22/tcp	346
2.36.2	Low general/icmp	347
2.37	192.168.0.131	348
2.37.1	Low general/icmp	348
2.37.2	Low 22/tcp	349
2.38	192.168.0.217	350
2.38.1	Low general/icmp	350
2.38.2	Low 22/tcp	351
2.39	192.168.0.234	352
2.39.1	Low 22/tcp	352
2.39.2	Low general/icmp	353
2.40	192.168.0.233	354
2.40.1	Low general/icmp	355
2.40.2	Low 22/tcp	356
2.41	192.168.0.232	357
2.41.1	Low general/icmp	357
2.41.2	Low 22/tcp	358
2.42	192.168.0.126	359
2.42.1	Low general/icmp	359
2.42.2	Low 22/tcp	360
2.43	192.168.0.248	361
2.43.1	Low 22/tcp	361
2.43.2	Low general/icmp	362
2.44	192.168.0.208	363
2.44.1	Low general/icmp	364
2.44.2	Low 22/tcp	365
2.45	192.168.0.211	366
2.45.1	Low general/icmp	366
2.45.2	Low 22/tcp	367
2.46	192.168.0.160	368
2.46.1	Low general/icmp	368
2.47	192.168.0.35	369
2.47.1	Low general/icmp	369
2.48	192.168.0.161	370
2.48.1	Low general/icmp	371

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.0.200 srvtelefonia.compwire.local	21	12	1	0	0
192.168.0.42 srvowncloud.compwire.local	4	10	2	0	0
192.168.0.6 srvsqlserver.compwire.local	0	3	0	0	0
192.168.0.241 srvwds.compwire.local	0	3	1	0	0
192.168.0.252	0	2	1	0	0
192.168.0.125 srvsaboia01.compwire.local	0	8	1	0	0
192.168.0.143 vb365.compwire.local	0	3	1	0	0
192.168.0.202 srvwsus.compwire.local	0	3	1	0	0
192.168.0.168 srvsapmigrate.compwire.local	0	3	1	0	0
192.168.0.250 srvveeam.compwire.local	0	3	1	0	0
192.168.0.65 srvdados.compwire.local	0	4	1	0	0
192.168.0.3 srvsap.compwire.local	0	3	1	0	0
192.168.0.220 accessclient.compwire.local	0	3	1	0	0
192.168.0.254	0	5	0	0	0
192.168.0.15 devcpwquotes.compwire.com.br	0	8	2	0	0
192.168.0.249 srvsalesbkip	0	2	1	0	0
192.168.0.201	0	2	2	0	0
192.168.0.2 srvsaphana	0	2	2	0	0
192.168.0.16 srvad02.compwire.local	0	1	1	0	0
192.168.0.142 srvdns02.compwire.local	0	3	2	0	0
192.168.0.5 srvsql.compwire.local	0	3	2	0	0
192.168.0.141 srvdns01.compwire.local	0	3	2	0	0
192.168.0.9 srvad01.compwire.local	0	1	1	0	0

... (continues) ...

... (continued) ...

Host	High	Medium	Low	Log	False Positive
192.168.0.209	0	1	2	0	0
192.168.0.106 srvview04.compwire.local	0	1	1	0	0
192.168.0.57 dspam.compwire.local	0	4	2	0	0
192.168.0.28 srvmonitoramento.compwire.local	0	3	2	0	0
192.168.0.99 srvview03.compwire.local	0	1	1	0	0
192.168.0.25 srvsap01.compwire.com.br	0	2	1	0	0
192.168.0.104 smtp1.spam.compwire.com.br	0	3	2	0	0
192.168.0.246 srvzabbixcpw.compwire.local	0	1	2	0	0
192.168.0.130	0	1	2	0	0
192.168.0.61 nodejs.compwire.com.br	0	1	2	0	0
192.168.0.97 srvuag01.compwire.com.br	0	1	0	0	0
192.168.0.245 srvzproxycpw.compwire.local	0	0	2	0	0
192.168.0.67	0	0	2	0	0
192.168.0.131	0	0	2	0	0
192.168.0.217 srvreport01.compwire.local	0	0	2	0	0
192.168.0.234	0	0	2	0	0
192.168.0.233	0	0	2	0	0
192.168.0.232	0	0	2	0	0
192.168.0.126 socnextgen01.compwire.local	0	0	2	0	0
192.168.0.248	0	0	2	0	0
192.168.0.208	0	0	2	0	0
192.168.0.211 srvappbkp.compwire.local	0	0	2	0	0
192.168.0.160 srvcameras2.compwire.local	0	0	1	0	0
192.168.0.35	0	0	1	0	0
192.168.0.161 srvcameras3.compwire.com.br	0	0	1	0	0
Total: 48	25	109	70	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 204 results selected by the filtering described above. Before filtering there were 2194 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.0.2 - srvsaphana	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 192.168.0.200

Host scan start Sun May 5 04:25:23 2024 UTC

Host scan end Sun May 5 05:35:09 2024 UTC

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

2.1.1 High 80/tcp

High (CVSS: 10.0)

NVT: Apache Tomcat End of Life (EOL) Detection - Windows

Product detection result

cpe:/a:apache:tomcat:7.0.61

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)

Summary

... continues on next page ...

...continued from previous page ...
The Apache Tomcat version on the remote host has reached the end of life (EOL) and should not be used anymore.
Quality of Detection: 80
Vulnerability Detection Result The "Apache Tomcat" version on the remote host has reached the end of life. CPE: cpe:/a:apache:tomcat:7.0.61 Installed version: 7.0.61 Location/URL: 80/tcp EOL version: 7.0 EOL date: 2021-03-31
Impact An EOL version of Apache Tomcat is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.
Solution: Solution type: VendorFix Update the Apache Tomcat version on the remote host to a still supported version.
Vulnerability Detection Method Checks if an EOL version is present on the target host. Details: Apache Tomcat End of Life (EOL) Detection - Windows OID:1.3.6.1.4.1.25623.1.0.108134 Version used: 2024-02-28T14:37:42Z
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References url: https://tomcat.apache.org/tomcat-10.0-eol.html url: https://tomcat.apache.org/tomcat-85-eol.html url: https://tomcat.apache.org/tomcat-80-eol.html url: https://tomcat.apache.org/tomcat-70-eol.html url: https://tomcat.apache.org/tomcat-60-eol.html url: https://tomcat.apache.org/tomcat-55-eol.html url: https://en.wikipedia.org/wiki/Apache_Tomcat#Releases url: https://tomcat.apache.org/whichversion.html

High (CVSS: 9.8)
NVT: Apache Tomcat Multiple Vulnerabilities (Feb 2020) - Windows
Product detection result cpe:/a:apache:tomcat:7.0.61 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to multiple vulnerabilities.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.100 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 7.0.100, 8.5.51, 9.0.31 or later.
Affected Software/OS Apache Tomcat 7.0.0 to 7.0.99, 8.5.0 to 8.5.50 and 9.0.0.M1 to 9.0.30.
Vulnerability Insight Apache Tomcat is prone to multiple vulnerabilities: - HTTP request smuggling vulnerability (CVE-2020-1935) - AJP Request Injection and potential Remote Code Execution dubbed 'Ghostcat' (CVE-2020-1938)
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Multiple Vulnerabilities (Feb 2020) - Windows OID:1.3.6.1.4.1.25623.1.0.143550 Version used: 2024-02-08T05:05:59Z
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
... continues on next page ...

...continued from previous page ...

References

cve: CVE-2020-1935
 cve: CVE-2020-1938
 cisa: Known Exploited Vulnerability (KEV) catalog
 url: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
 url: <https://lists.apache.org/thread.html/r127f76181aceffea2bd4711b03c595d0f115f>
 ↪63e020348fe925a916c%40%3Cannounce.tomcat.apache.org%3E
 url: <https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1>
 ↪a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E
 url: <https://www.chaitin.cn/en/ghostcat>
 url: <https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487>
 url: <https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi>
 url: <https://tomcat.apache.org/tomcat-7.0-doc/changelog.html>
 url: <https://tomcat.apache.org/tomcat-8.5-doc/changelog.html>
 url: <https://tomcat.apache.org/tomcat-9.0-doc/changelog.html>
 cert-bund: WID-SEC-2024-0528
 cert-bund: WID-SEC-2023-2480
 cert-bund: WID-SEC-2023-2130
 dfn-cert: DFN-CERT-2021-1736
 dfn-cert: DFN-CERT-2021-0575
 dfn-cert: DFN-CERT-2020-2482
 dfn-cert: DFN-CERT-2020-1707
 dfn-cert: DFN-CERT-2020-1706
 dfn-cert: DFN-CERT-2020-1508
 dfn-cert: DFN-CERT-2020-1413
 dfn-cert: DFN-CERT-2020-1276
 dfn-cert: DFN-CERT-2020-1134
 dfn-cert: DFN-CERT-2020-0850
 dfn-cert: DFN-CERT-2020-0835
 dfn-cert: DFN-CERT-2020-0821
 dfn-cert: DFN-CERT-2020-0569
 dfn-cert: DFN-CERT-2020-0557
 dfn-cert: DFN-CERT-2020-0501
 dfn-cert: DFN-CERT-2020-0381

High (CVSS: 9.1)

NVT: Apache Tomcat 'SecurityManager' Information Disclosure Vulnerability - Windows

Product detection result

cpe:/a:apache:tomcat:7.0.61
 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
 ↪7652)

Summary

... continues on next page ...

...continued from previous page ...
Apache Tomcat is prone to an information disclosure vulnerability.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.76 Installation path / port: 80/tcp
Impact Successful exploitation will allow remote attackers to obtain sensitive information from requests other than their own.
Solution: Solution type: VendorFix Upgrade to version 9.0.0.M18, 8.5.12, 8.0.42, 7.0.76 or later.
Affected Software/OS Apache Tomcat versions 9.0.0.M1 to 9.0.0.M17, Apache Tomcat versions 8.5.0 to 8.5.11, Apache Tomcat versions 8.0.0.RC1 to 8.0.41 and Apache Tomcat versions 7.0.0 to 7.0.75 on Windows
Vulnerability Insight A some calls to application listeners did not use the appropriate facade object. When running an untrusted application under a SecurityManager, it was therefore possible for that untrusted application to retain a reference to the request or response object and thereby access and/or modify information associated with another web application.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat 'SecurityManager' Information Disclosure Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.810764 Version used: 2024-02-15T05:05:40Z
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2017-5648 url: http://tomcat.apache.org/security-9.html url: http://tomcat.apache.org/security-8.html
... continues on next page ...

...continued from previous page ...
url: http://tomcat.apache.org/security-7.html
url: http://lists.apache.org/thread.html/d0e00f2e147a9e9b13a6829133092f349b2882b↵f6860397368a52600@%3Cannounce.tomcat.apache.org%3E
cert-bund: WID-SEC-2024-0528
cert-bund: CB-K18/0047
cert-bund: CB-K17/1257
cert-bund: CB-K17/1246
cert-bund: CB-K17/1060
cert-bund: CB-K17/0801
cert-bund: CB-K17/0604
dfn-cert: DFN-CERT-2018-0051
dfn-cert: DFN-CERT-2017-1300
dfn-cert: DFN-CERT-2017-1288
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-0828
dfn-cert: DFN-CERT-2017-0624

High (CVSS: 9.1)
NVT: Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities - Windows
Product detection result cpe:/a:apache:tomcat:7.0.61 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10↵7652)
Summary Apache Tomcat is prone to security bypass and information disclosure vulnerabilities.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.72 Installation path / port: 80/tcp
Impact Successful exploitation will allow remote attackers to gain access to potentially sensitive information and bypass certain security restrictions.
Solution: Solution type: VendorFix Upgrade to Apache Tomcat version 9.0.0.M10 or 8.5.5 or 8.0.37 or 7.0.72 or 6.0.47 or later.
... continues on next page ...

...continued from previous page ...	
Affected Software/OS Apache Tomcat versions 9.0.0.M1 to 9.0.0.M9, Apache Tomcat versions 8.5.0 to 8.5.4, Apache Tomcat versions 8.0.0.RC1 to 8.0.36, Apache Tomcat versions 7.0.0 to 7.0.70, and Apache Tomcat versions 6.0.0 to 6.0.45 on Windows.	
Vulnerability Insight Multiple flaws exist due to: <ul style="list-style-type: none">- An error in the system property replacement feature for configuration files.- An error in the realm implementations in Apache Tomcat that does not process the supplied password if the supplied user name did not exist.- An error in the configured SecurityManager via a Tomcat utility method that is accessible to web applications.- An error in the configured SecurityManager via manipulation of the configuration parameters for the JSP Servlet.- An error in the ResourceLinkFactory implementation in Apache Tomcat that does not limit web application access to global JNDI resources to those resources explicitly linked to the web application.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities - Wind. ↔.. OID:1.3.6.1.4.1.25623.1.0.811298 Version used: 2024-02-15T05:05:40Z	
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)	
References cve: CVE-2016-6794 cve: CVE-2016-0762 cve: CVE-2016-5018 cve: CVE-2016-6796 cve: CVE-2016-6797 url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.72 url: http://www.securityfocus.com/bid/93940 url: http://www.securityfocus.com/bid/93944 url: http://www.securityfocus.com/bid/93939 url: http://www.securityfocus.com/bid/93942 url: http://www.securityfocus.com/bid/93943 url: http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.47 url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M10	
...continues on next page ...	

...continued from previous page ...
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.5_and_8.5.6
cert-bund: WID-SEC-2022-1910
cert-bund: CB-K17/1060
cert-bund: CB-K17/1033
cert-bund: CB-K17/1031
cert-bund: CB-K17/0659
cert-bund: CB-K17/0397
cert-bund: CB-K17/0133
cert-bund: CB-K16/1927
cert-bund: CB-K16/1673
cert-bund: CB-K16/1646
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-1068
dfn-cert: DFN-CERT-2017-1064
dfn-cert: DFN-CERT-2017-0673
dfn-cert: DFN-CERT-2017-0404
dfn-cert: DFN-CERT-2017-0137
dfn-cert: DFN-CERT-2016-2035
dfn-cert: DFN-CERT-2016-1772
dfn-cert: DFN-CERT-2016-1743

High (CVSS: 8.8)

NVT: Apache Tomcat CSRF Token Leak Vulnerability (Feb 2016) - Windows

Product detection result

cpe:/a:apache:tomcat:7.0.61

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
 ↪7652)

Summary

Apache Tomcat is prone to a CSRF Token leak vulnerability.

Quality of Detection: 80

Vulnerability Detection Result

Installed version: 7.0.61

Fixed version: 7.0.68

Installation

path / port: 80/tcp

Impact

... continues on next page ...

...continued from previous page ...
Successful exploitation will allow remote attackers to bypass a CSRF protection mechanism by using a token.
Solution: Solution type: VendorFix Upgrade to version 7.0.68, or 8.0.32 or 9.0.0.M3 or later.
Affected Software/OS Apache Tomcat 7.0.1 before 7.0.68, 8.0.0.RC1 before 8.0.32, and 9.0.0.M1 on Windows.
Vulnerability Insight The flaw is due to an error in index page of the Manager and Host Manager applications included a valid CSRF token when issuing a redirect .
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat CSRF Token Leak Vulnerability (Feb 2016) - Windows OID:1.3.6.1.4.1.25623.1.0.807405 Version used: 2024-02-08T05:05:59Z
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2015-5351 url: http://tomcat.apache.org/security-9.html url: http://www.securityfocus.com/bid/83330 url: http://tomcat.apache.org/security-8.html url: http://tomcat.apache.org/security-7.html cert-bund: CB-K17/1750 cert-bund: CB-K17/0661 cert-bund: CB-K17/0098 cert-bund: CB-K16/1799 cert-bund: CB-K16/1758 cert-bund: CB-K16/1622 cert-bund: CB-K16/0993 cert-bund: CB-K16/0789 cert-bund: CB-K16/0758 cert-bund: CB-K16/0476 cert-bund: CB-K16/0292 dfn-cert: DFN-CERT-2017-1821 dfn-cert: DFN-CERT-2017-0677 dfn-cert: DFN-CERT-2017-0090
... continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2016-1905
dfn-cert: DFN-CERT-2016-1823
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1059
dfn-cert: DFN-CERT-2016-0842
dfn-cert: DFN-CERT-2016-0807
dfn-cert: DFN-CERT-2016-0518
dfn-cert: DFN-CERT-2016-0314
```

High (CVSS: 8.8)

NVT: Apache Tomcat Security Manager Bypass Vulnerability - 01 (Feb 2016) - Windows

Product detection result

cpe:/a:apache:tomcat:7.0.61

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)**Summary**

Apache Tomcat is prone to a security manager bypass vulnerability.

Quality of Detection: 80**Vulnerability Detection Result**

Installed version: 7.0.61

Fixed version: 7.0.68

Installation

path / port: 80/tcp

Impact

Successful exploitation will allow remote authenticated users to bypass intended SecurityManager restrictions and execute arbitrary code in a privileged context and read arbitrary HTTP requests, and consequently discover session ID values.

Solution:**Solution type:** VendorFix

Upgrade to version 6.0.45 or 7.0.68 or 8.0.32 or 9.0.0.M3 or later.

Affected Software/OS

Apache Tomcat 6.0.0 before 6.0.45, and 7.0.0 before 7.0.68, 8.0.0.RC1 before 8.0.31, and 9.0.0.M1 on Windows.

Vulnerability Insight

... continues on next page ...

...continued from previous page ...
The flaw exists due to an improper validation of several session persistence mechanisms and the StatusManagerServlet loaded by a web application when a security manager was configured.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Security Manager Bypass Vulnerability - 01 (Feb 2016) - Windows OID: 1.3.6.1.4.1.25623.1.0.807408 Version used: 2024-02-08T05:05:59Z
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2016-0714 cve: CVE-2016-0706 url: http://tomcat.apache.org/security-9.html url: http://www.securityfocus.com/bid/83324 url: http://www.securityfocus.com/bid/83327 url: http://tomcat.apache.org/security-8.html url: http://tomcat.apache.org/security-7.html cert-bund: CB-K17/1750 cert-bund: CB-K17/0661 cert-bund: CB-K17/0098 cert-bund: CB-K16/1799 cert-bund: CB-K16/1758 cert-bund: CB-K16/1630 cert-bund: CB-K16/1622 cert-bund: CB-K16/1568 cert-bund: CB-K16/0993 cert-bund: CB-K16/0789 cert-bund: CB-K16/0758 cert-bund: CB-K16/0496 cert-bund: CB-K16/0476 cert-bund: CB-K16/0292 dfn-cert: DFN-CERT-2017-1821 dfn-cert: DFN-CERT-2017-0677 dfn-cert: DFN-CERT-2017-0090 dfn-cert: DFN-CERT-2016-1905 dfn-cert: DFN-CERT-2016-1823 dfn-cert: DFN-CERT-2016-1726 dfn-cert: DFN-CERT-2016-1715 dfn-cert: DFN-CERT-2016-1661 dfn-cert: DFN-CERT-2016-1059 dfn-cert: DFN-CERT-2016-0842
...continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2016-0807
dfn-cert: DFN-CERT-2016-0537
dfn-cert: DFN-CERT-2016-0518
dfn-cert: DFN-CERT-2016-0314
```

High (CVSS: 8.1)

NVT: Apache Tomcat RCE Vulnerability (Apr 2019) - Windows

Product detection result

cpe:/a:apache:tomcat:7.0.61

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)**Summary**

Apache Tomcat is prone to a remote code execution vulnerability due to a bug in the way the JRE passes command line arguments to Windows.

Quality of Detection: 80**Vulnerability Detection Result**

Installed version: 7.0.61

Fixed version: 7.0.94

Installation

path / port: 80/tcp

Solution:**Solution type:** VendorFix

Update to version 7.0.94, 8.5.40, 9.0.19 or later.

Affected Software/OS

Apache Tomcat 7.0.0 to 7.0.93, 8.5.0 to 8.5.39 and 9.0.0.M1 to 9.0.17.

Vulnerability Insight

When running on Windows with enableCmdLineArguments enabled, the CGI Servlet is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option enableCmdLineArguments is disabled by default in Tomcat.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: Apache Tomcat RCE Vulnerability (Apr 2019) - Windows

OID:1.3.6.1.4.1.25623.1.0.142265

... continues on next page ...

...continued from previous page ...
Version used: 2024-02-08T14:36:53Z
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2019-0232 url: http://tomcat.apache.org/security-9.html url: http://tomcat.apache.org/security-8.html url: http://tomcat.apache.org/security-7.html cert-bund: WID-SEC-2024-0528 cert-bund: CB-K19/0920 cert-bund: CB-K19/0616 cert-bund: CB-K19/0306 dfn-cert: DFN-CERT-2019-1398 dfn-cert: DFN-CERT-2019-0732

High (CVSS: 8.1)
NVT: Apache Tomcat Session Fixation Vulnerability (Feb 2016) - Windows
Product detection result cpe:/a:apache:tomcat:7.0.61 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to a Session Fixation Vulnerability.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.66 Installation path / port: 80/tcp
Impact Successful exploitation will allow remote attackers to hijack web sessions by leveraging use of a requestedSessionSSL field for an unintended request.
Solution: ... continues on next page ...

...continued from previous page...	
Solution type: VendorFix	Upgrade to version 7.0.66 or 8.0.32 or 9.0.0.M3 or later.
Affected Software/OS	Apache Tomcat 7.0.5 before 7.0.66, 8.0.0.RC1 before 8.0.31, and 9.0.0.M1 on Windows.
Vulnerability Insight	The flaw exists due to insufficient recycling of the requestedSessionSSL field.
Vulnerability Detection Method	Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Session Fixation Vulnerability (Feb 2016) - Windows OID:1.3.6.1.4.1.25623.1.0.807409 Version used: 2024-02-08T05:05:59Z
Product Detection Result	Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References	cve: CVE-2015-5346 url: http://tomcat.apache.org/security-9.html url: http://www.securityfocus.com/bid/83323 url: http://tomcat.apache.org/security-6.html url: http://tomcat.apache.org/security-7.html cert-bund: CB-K16/1799 cert-bund: CB-K16/1630 cert-bund: CB-K16/1568 cert-bund: CB-K16/0993 cert-bund: CB-K16/0789 cert-bund: CB-K16/0758 cert-bund: CB-K16/0476 cert-bund: CB-K16/0292 dfn-cert: DFN-CERT-2016-1905 dfn-cert: DFN-CERT-2016-1726 dfn-cert: DFN-CERT-2016-1661 dfn-cert: DFN-CERT-2016-1059 dfn-cert: DFN-CERT-2016-0842 dfn-cert: DFN-CERT-2016-0807 dfn-cert: DFN-CERT-2016-0518 dfn-cert: DFN-CERT-2016-0314

High (CVSS: 7.5)
NVT: Apache Tomcat DoS Vulnerability (Feb 2023) - Windows
Product detection result cpe:/a:apache:tomcat:7.0.61 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to a denial of service (DoS) vulnerability.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 8.5.85 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 8.5.85, 9.0.71, 10.1.5, 11.0.0-M3 or later.
Affected Software/OS Apache Tomcat versions through 8.5.84, 9.0.0-M1 through 9.0.70, 10.x through 10.1.4 and 11.0.0-M1 only.
Vulnerability Insight Apache Tomcat uses a packaged renamed copy of Apache Commons FileUpload to provide the file upload functionality defined in the Jakarta Servlet specification. Apache Tomcat was, therefore, also vulnerable to the Apache Commons FileUpload vulnerability CVE-2023-24998 as there was no limit to the number of request parts processed. This resulted in the possibility of an attacker triggering a DoS with a malicious upload or series of uploads.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat DoS Vulnerability (Feb 2023) - Windows OID:1.3.6.1.4.1.25623.1.0.104551 Version used: 2023-10-12T05:05:32Z
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2023-24998 url: https://lists.apache.org/thread/g16kv0xpp272htz107molwbbgdrqrdk1 url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M3 url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.5 url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.71 url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.85 url: https://lists.apache.org/thread/4xl4l09mhwg4vgsk7dxqogcjrobrrdoy cert-bund: WID-SEC-2024-0124 cert-bund: WID-SEC-2024-0117 cert-bund: WID-SEC-2024-0054 cert-bund: WID-SEC-2023-2688 cert-bund: WID-SEC-2023-2675 cert-bund: WID-SEC-2023-2674 cert-bund: WID-SEC-2023-2625 cert-bund: WID-SEC-2023-2309 cert-bund: WID-SEC-2023-2031 cert-bund: WID-SEC-2023-1817 cert-bund: WID-SEC-2023-1815 cert-bund: WID-SEC-2023-1813 cert-bund: WID-SEC-2023-1812 cert-bund: WID-SEC-2023-1811 cert-bund: WID-SEC-2023-1809 cert-bund: WID-SEC-2023-1808 cert-bund: WID-SEC-2023-1807 cert-bund: WID-SEC-2023-1794 cert-bund: WID-SEC-2023-1792 cert-bund: WID-SEC-2023-1791 cert-bund: WID-SEC-2023-1784 cert-bund: WID-SEC-2023-1783 cert-bund: WID-SEC-2023-1782 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-1142 cert-bund: WID-SEC-2023-1021 cert-bund: WID-SEC-2023-1017 cert-bund: WID-SEC-2023-1016 cert-bund: WID-SEC-2023-1012 cert-bund: WID-SEC-2023-1007 cert-bund: WID-SEC-2023-1005 cert-bund: WID-SEC-2023-0609 cert-bund: WID-SEC-2023-0433 dfn-cert: DFN-CERT-2024-0059 dfn-cert: DFN-CERT-2024-0048 dfn-cert: DFN-CERT-2023-2778
...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2023-2545
dfn-cert: DFN-CERT-2023-2469
dfn-cert: DFN-CERT-2023-2054
dfn-cert: DFN-CERT-2023-1648
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2023-1642
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1362
dfn-cert: DFN-CERT-2023-1109
dfn-cert: DFN-CERT-2023-0902
dfn-cert: DFN-CERT-2023-0886
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2023-0763
dfn-cert: DFN-CERT-2023-0574
dfn-cert: DFN-CERT-2023-0540
dfn-cert: DFN-CERT-2023-0414

High (CVSS: 7.5)
NVT: Apache Tomcat 'MultipartStream' Class DoS Vulnerability - Windows
Product detection result cpe:/a:apache:tomcat:7.0.61 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to a denial of service (DoS) vulnerability.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.70 Installation path / port: 80/tcp
Impact Successful exploitation will allow remote attackers to cause a denial of service (CPU consumption).
Solution: Solution type: VendorFix Upgrade to version 7.0.70, or 8.0.36, or 8.5.3, or 9.0.0.M7, or later.
... continues on next page ...

...continued from previous page ...
<p>Affected Software/OS Apache Tomcat 7.x before 7.0.70, 8.0.0.RC1 before 8.0.36, 8.5.x before 8.5.3, and 9.0.0.M1 before 9.0.0.M7.</p>
<p>Vulnerability Insight The flaw is due to an error in the 'MultipartStream' class in Apache Commons Fileupload when processing multi-part requests.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat 'MultipartStream' Class DoS Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.808197 Version used: 2022-04-13T13:17:10Z</p>
<p>Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)</p>
<p>References cve: CVE-2016-3092 url: http://tomcat.apache.org/security-7.html url: http://www.securityfocus.com/bid/91453 url: http://tomcat.apache.org/security-8.html url: http://tomcat.apache.org/security-9.html cert-bund: WID-SEC-2023-0644 cert-bund: WID-SEC-2022-1537 cert-bund: WID-SEC-2022-1375 cert-bund: CB-K18/0605 cert-bund: CB-K17/1750 cert-bund: CB-K17/1198 cert-bund: CB-K17/1060 cert-bund: CB-K17/0657 cert-bund: CB-K17/0397 cert-bund: CB-K16/1993 cert-bund: CB-K16/1799 cert-bund: CB-K16/1758 cert-bund: CB-K16/1322 cert-bund: CB-K16/1002 cert-bund: CB-K16/0993 dfn-cert: DFN-CERT-2023-0574 dfn-cert: DFN-CERT-2018-2554 dfn-cert: DFN-CERT-2018-0729 dfn-cert: DFN-CERT-2017-1821</p>
...continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0404
dfn-cert: DFN-CERT-2016-2104
dfn-cert: DFN-CERT-2016-1905
dfn-cert: DFN-CERT-2016-1823
dfn-cert: DFN-CERT-2016-1407
dfn-cert: DFN-CERT-2016-1068
dfn-cert: DFN-CERT-2016-1059
```

High (CVSS: 7.5)

NVT: Apache Tomcat 'Hostname Verification' Security Bypass Vulnerability - Windows

Product detection result

cpe:/a:apache:tomcat:7.0.61

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)**Summary**

Apache Tomcat is prone to a security bypass vulnerability.

Quality of Detection: 80**Vulnerability Detection Result**

Installed version: 7.0.61

Fixed version: 7.0.90

Installation

path / port: 80/tcp

Impact

Successful exploitation will allow an attacker to bypass certain security restrictions and perform unauthorized actions.

Solution:**Solution type:** VendorFix

Upgrade to Apache Tomcat version 9.0.10 or 8.5.32 or 8.0.53 or 7.0.90 or later. Please see the references for more information.

Affected Software/OS

Apache Tomcat versions 9.0.0.M1 to 9.0.9, 8.5.0 to 8.5.31, 8.0.0.RC1 to 8.0.52 and 7.0.35 to 7.0.88 on Windows.

... continues on next page ...

...continued from previous page...	
Vulnerability Insight	
The flaw exists due to a missing host name verification when using TLS with the WebSocket client.	
Vulnerability Detection Method	
Checks if a vulnerable version is present on the target host. Details: Apache Tomcat 'Hostname Verification' Security Bypass Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.813742 Version used: 2024-02-15T05:05:40Z	
Product Detection Result	
Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)	
References	
cve: CVE-2018-8034 url: http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C20180722091057.GA70283@minotaur.apache.org%3E url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.10 url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.53 url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.32 url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.90 cert-bund: WID-SEC-2024-0528 cert-bund: CB-K19/0907 cert-bund: CB-K19/0616 cert-bund: CB-K19/0320 cert-bund: CB-K18/1005 cert-bund: CB-K18/0809 dfn-cert: DFN-CERT-2019-2418 dfn-cert: DFN-CERT-2019-1627 dfn-cert: DFN-CERT-2019-1237 dfn-cert: DFN-CERT-2019-0951 dfn-cert: DFN-CERT-2019-0451 dfn-cert: DFN-CERT-2019-0147 dfn-cert: DFN-CERT-2018-2165 dfn-cert: DFN-CERT-2018-2142 dfn-cert: DFN-CERT-2018-1753 dfn-cert: DFN-CERT-2018-1471 dfn-cert: DFN-CERT-2018-1443 dfn-cert: DFN-CERT-2018-1262	

High (CVSS: 7.5)
NVT: Apache Tomcat 'VirtualDirContext' Information Disclosure Vulnerability - Windows
Product detection result cpe:/a:apache:tomcat:7.0.61 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to an information disclosure vulnerability.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.81 Installation path / port: 80/tcp
Impact Successful exploitation will allow remote attackers to obtain potentially sensitive information on the target system.
Solution: Solution type: VendorFix Upgrade to Tomcat version 7.0.81 or later.
Affected Software/OS Apache Tomcat versions 7.0.0 to 7.0.80 on Windows
Vulnerability Insight The flaw is due to an improper serving of files via 'VirtualDirContext'.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat 'VirtualDirContext' Information Disclosure Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.811846 Version used: 2024-02-15T05:05:40Z
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
... continues on next page ...

...continued from previous page ...

References

cve: CVE-2017-12616
 url: <http://www.securitytracker.com/id/1039393>
 url: <http://www.securityfocus.com/bid/100897>
 url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.81
 cert-bund: CB-K18/0420
 cert-bund: CB-K17/2024
 cert-bund: CB-K17/1593
 dfn-cert: DFN-CERT-2018-1253
 dfn-cert: DFN-CERT-2018-1038
 dfn-cert: DFN-CERT-2018-0455
 dfn-cert: DFN-CERT-2017-2116
 dfn-cert: DFN-CERT-2017-1665

High (CVSS: 7.5)

NVT: Apache Tomcat 'UTF-8 Decoder' Denial of Service Vulnerability - Windows

Product detection result

cpe:/a:apache:tomcat:7.0.61
 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
 ↪7652)

Summary

Apache Tomcat is prone to a denial of service (DoS) vulnerability.

Quality of Detection: 80**Vulnerability Detection Result**

Installed version: 7.0.61
 Fixed version: 7.0.90
 Installation
 path / port: 80/tcp

Impact

Successful exploitation will allow an attacker to conduct a denial-of-service condition.

Solution:**Solution type:** VendorFix

Upgrade to Apache Tomcat version 9.0.8 or 8.5.31 or 8.0.52 or 7.0.90 or later. Please see the references for more information.

Affected Software/OS

... continues on next page ...

...continued from previous page ...
Apache Tomcat 9.0.0.M9 to 9.0.7 Apache Tomcat 8.5.0 to 8.5.30 Apache Tomcat 8.0.0.RC1 to 8.0.51 Apache Tomcat 7.0.28 to 7.0.86 on Windows.
Vulnerability Insight The flaw exists due to improper handling of overflow in the UTF-8 decoder with supplementary characters.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat 'UTF-8 Decoder' Denial of Service Vulnerability - Windows OID: 1.3.6.1.4.1.25623.1.0.813724 Version used: 2024-02-15T05:05:40Z
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2018-1336 url: http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C20180722090435.GA60759%40minotaur.apache.org%3E url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.8 url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.31 url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.52 cert-bund: WID-SEC-2024-0528 cert-bund: CB-K18/0809 dfn-cert: DFN-CERT-2020-0048 dfn-cert: DFN-CERT-2018-2474 dfn-cert: DFN-CERT-2018-2165 dfn-cert: DFN-CERT-2018-2142 dfn-cert: DFN-CERT-2018-2133 dfn-cert: DFN-CERT-2018-2125 dfn-cert: DFN-CERT-2018-2097 dfn-cert: DFN-CERT-2018-1928 dfn-cert: DFN-CERT-2018-1753 dfn-cert: DFN-CERT-2018-1541 dfn-cert: DFN-CERT-2018-1471 dfn-cert: DFN-CERT-2018-1443 dfn-cert: DFN-CERT-2018-1262

High (CVSS: 7.5)
NVT: Apache Tomcat Security Bypass Vulnerability - Windows
Product detection result cpe:/a:apache:tomcat:7.0.61 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to a security bypass vulnerability.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.78 Installation path / port: 80/tcp
Impact Successful exploitation will allow an attacker to exploit this issue to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.
Solution: Solution type: VendorFix Upgrade to version 9.0.0.M21, or 8.5.15, or 8.0.44, or 7.0.78 or later.
Affected Software/OS Apache Tomcat 9.0.0.M1 to 9.0.0.M20, Apache Tomcat 8.5.0 to 8.5.14, Apache Tomcat 8.0.0.RC1 to 8.0.43 and Apache Tomcat 7.0.0 to 7.0.77 on Windows
Vulnerability Insight The error page mechanism of the Java Servlet Specification requires that, when an error occurs and an error page is configured for the error that occurred, the original request and response are forwarded to the error page. This means that the request is presented to the error page with the original HTTP method. If the error page is a static file, expected behaviour is to serve content of the file as if processing a GET request, regardless of the actual HTTP method. Tomcat's Default Servlet did not do this. Depending on the original request this could lead to unexpected and undesirable results for static error pages including, if the DefaultServlet is configured to permit writes, the replacement or removal of the custom error page
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Security Bypass Vulnerability - Windows
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.811140 Version used: 2024-02-15T05:05:40Z
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2017-5664 url: https://lists.apache.org/thread.html/a42c48e37398d76334e17089e43ccab945238b↪8b7896538478d760660%3Cannounce.tomcat.apache.org%3E url: http://www.securityfocus.com/bid/98888 cert-bund: WID-SEC-2024-0528 cert-bund: CB-K18/0605 cert-bund: CB-K18/0603 cert-bund: CB-K18/0478 cert-bund: CB-K18/0066 cert-bund: CB-K18/0047 cert-bund: CB-K17/2024 cert-bund: CB-K17/2017 cert-bund: CB-K17/1831 cert-bund: CB-K17/1748 cert-bund: CB-K17/1492 cert-bund: CB-K17/1423 cert-bund: CB-K17/1257 cert-bund: CB-K17/1246 cert-bund: CB-K17/0977 dfn-cert: DFN-CERT-2018-1274 dfn-cert: DFN-CERT-2018-0729 dfn-cert: DFN-CERT-2018-0513 dfn-cert: DFN-CERT-2018-0077 dfn-cert: DFN-CERT-2018-0051 dfn-cert: DFN-CERT-2017-2116 dfn-cert: DFN-CERT-2017-2106 dfn-cert: DFN-CERT-2017-1914 dfn-cert: DFN-CERT-2017-1827 dfn-cert: DFN-CERT-2017-1558 dfn-cert: DFN-CERT-2017-1485 dfn-cert: DFN-CERT-2017-1300 dfn-cert: DFN-CERT-2017-1288 dfn-cert: DFN-CERT-2017-1011

High (CVSS: 7.5)
NVT: Apache Tomcat 'pipelined' Requests Information Disclosure Vulnerability - Windows
Product detection result cpe:/a:apache:tomcat:7.0.61 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to an information disclosure vulnerability.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.77 Installation path / port: 80/tcp
Impact Successful exploitation will allow remote attackers to obtain sensitive information from requests other than their own.
Solution: Solution type: VendorFix Upgrade to version 9.0.0.M19, 8.5.13, 8.0.43, 7.0.77, 6.0.53 or later.
Affected Software/OS Apache Tomcat versions 9.0.0.M1 to 9.0.0.M18, Apache Tomcat versions 8.5.0 to 8.5.12, Apache Tomcat versions 8.0.0.RC1 to 8.0.42, Apache Tomcat versions 7.0.0 to 7.0.76 and Apache Tomcat versions 6.0.0 to 6.0.52 on Windows.
Vulnerability Insight A bug in the handling of the pipelined requests when send file was used resulted in the pipelined request being lost when send file processing of the previous request completed.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat 'pipelined' Requests Information Disclosure Vulnerability - Windo. ↪.. OID:1.3.6.1.4.1.25623.1.0.810762 Version used: 2024-02-15T05:05:40Z
Product Detection Result ... continues on next page ...

...continued from previous page ...
Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2017-5647 url: http://tomcat.apache.org/security-9.html url: http://tomcat.apache.org/security-8.html url: http://tomcat.apache.org/security-7.html url: http://tomcat.apache.org/security-6.html url: https://lists.apache.org/thread.html/5796678c5a773c6f3ff57c178ac247d85ceca0 ↪dee9190ba48171451a0%3Cusers.tomcat.apache.org%3E cert-bund: WID-SEC-2024-0528 cert-bund: CB-K18/0047 cert-bund: CB-K17/1831 cert-bund: CB-K17/1423 cert-bund: CB-K17/1246 cert-bund: CB-K17/1205 cert-bund: CB-K17/1060 cert-bund: CB-K17/1033 cert-bund: CB-K17/0801 cert-bund: CB-K17/0604 dfn-cert: DFN-CERT-2018-0051 dfn-cert: DFN-CERT-2017-1914 dfn-cert: DFN-CERT-2017-1485 dfn-cert: DFN-CERT-2017-1288 dfn-cert: DFN-CERT-2017-1243 dfn-cert: DFN-CERT-2017-1095 dfn-cert: DFN-CERT-2017-1068 dfn-cert: DFN-CERT-2017-0828 dfn-cert: DFN-CERT-2017-0624

High (CVSS: 7.5)

NVT: Apache Tomcat NIO HTTP connector Information Disclosure Vulnerability - Windows

Product detection result

cpe:/a:apache:tomcat:7.0.61
 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
 ↪7652)

Summary

Apache Tomcat is prone to an information disclosure vulnerability.

...continues on next page ...

...continued from previous page ...	
Quality of Detection: 80	
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.75 Installation path / port: 80/tcp	
Impact Successful exploitation will allow remote attackers to gain access to potentially sensitive information.	
Solution: Solution type: VendorFix Upgrade to Apache Tomcat version 9.0.0.M15 or 8.5.9 or 8.0.41 or 7.0.75 or 6.0.50 or later.	
Affected Software/OS Apache Tomcat versions 9.0.0.M1 to 9.0.0.M13, Apache Tomcat versions 8.5.0 to 8.5.8, Apache Tomcat versions 8.0.0.RC1 to 8.0.39, Apache Tomcat versions 7.0.0 to 7.0.73, and Apache Tomcat versions 6.0.16 to 6.0.48 on Windows.	
Vulnerability Insight The flaw exists due to error handling of the send file code for the NIO HTTP connector in Apache Tomcat resulting in the current Processor object being added to the Processor cache multiple times. This in turn means that the same Processor could be used for concurrent requests. Sharing a Processor can result in information leakage between requests including, not not limited to, session ID and the response body.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat NIO HTTP connector Information Disclosure Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.811296 Version used: 2024-02-15T05:05:40Z	
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)	
References cve: CVE-2016-8745 url: https://bz.apache.org/bugzilla/show_bug.cgi?id=60409 url: http://www.securityfocus.com/bid/94828 url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M15 url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.41	
... continues on next page ...	

...continued from previous page...
url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.75
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.9
url: http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.50
cert-bund: WID-SEC-2024-0528
cert-bund: WID-SEC-2022-1375
cert-bund: CB-K18/0605
cert-bund: CB-K17/1746
cert-bund: CB-K17/1060
cert-bund: CB-K17/1033
cert-bund: CB-K17/0801
cert-bund: CB-K17/0444
cert-bund: CB-K17/0397
cert-bund: CB-K17/0303
cert-bund: CB-K17/0133
cert-bund: CB-K17/0090
cert-bund: CB-K16/1929
dfn-cert: DFN-CERT-2018-0729
dfn-cert: DFN-CERT-2017-1822
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-1068
dfn-cert: DFN-CERT-2017-0828
dfn-cert: DFN-CERT-2017-0456
dfn-cert: DFN-CERT-2017-0404
dfn-cert: DFN-CERT-2017-0308
dfn-cert: DFN-CERT-2017-0137
dfn-cert: DFN-CERT-2017-0095
dfn-cert: DFN-CERT-2016-2037

High (CVSS: 7.5)
NVT: Apache Tomcat Session Fixation Vulnerability (Dec 2019) - Windows
Product detection result cpe:/a:apache:tomcat:7.0.61 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to a session fixation vulnerability.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.99
...continues on next page...

...continued from previous page ...	
Installation	
path / port:	80/tcp
Solution:	
Solution type: VendorFix	
Update to version 7.0.99, 8.5.50, 9.0.30 or later.	
Affected Software/OS	
Apache Tomcat 7.0.0 to 7.0.98, 8.5.0 to 8.5.49 and 9.0.0.M1 to 9.0.29.	
Vulnerability Insight	
When using FORM authentication there was a narrow window where an attacker could perform a session fixation attack. The window was considered too narrow for an exploit to be practical but, erring on the side of caution, this issue has been treated as a security vulnerability.	
Vulnerability Detection Method	
Checks if a vulnerable version is present on the target host.	
Details: Apache Tomcat Session Fixation Vulnerability (Dec 2019) - Windows	
OID:1.3.6.1.4.1.25623.1.0.143314	
Version used: 2024-02-08T05:05:59Z	
Product Detection Result	
Product: cpe:/a:apache:tomcat:7.0.61	
Method: Apache Tomcat Detection Consolidation	
OID: 1.3.6.1.4.1.25623.1.0.107652)	
References	
cve: CVE-2019-17563	
url: https://lists.apache.org/thread.html/8b4c1db8300117b28a0f3f743c0b9e3f964687↪a690cdf9662a884bbd%40%3Cannounce.tomcat.apache.org%3E	
cert-bund: WID-SEC-2024-0528	
cert-bund: WID-SEC-2023-1229	
cert-bund: WID-SEC-2023-1049	
cert-bund: CB-K21/0071	
cert-bund: CB-K19/1102	
dfn-cert: DFN-CERT-2021-0575	
dfn-cert: DFN-CERT-2020-2132	
dfn-cert: DFN-CERT-2020-1134	
dfn-cert: DFN-CERT-2020-1129	
dfn-cert: DFN-CERT-2020-0821	
dfn-cert: DFN-CERT-2020-0780	
dfn-cert: DFN-CERT-2020-0775	
dfn-cert: DFN-CERT-2020-0557	
dfn-cert: DFN-CERT-2020-0501	
dfn-cert: DFN-CERT-2020-0345	
... continues on next page ...	

...continued from previous page ...

dfn-cert: DFN-CERT-2020-0027
 dfn-cert: DFN-CERT-2019-2710
 dfn-cert: DFN-CERT-2019-2673

High (CVSS: 7.1)

NVT: Apache Tomcat HTTP Request Line Information Disclosure Vulnerability - Windows

Product detection result

cpe:/a:apache:tomcat:7.0.61

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
 ↪7652)**Summary**

Apache Tomcat is prone to an information disclosure vulnerability.

Quality of Detection: 80**Vulnerability Detection Result**

Installed version: 7.0.61

Fixed version: 7.0.73

Installation

path / port: 80/tcp

Impact

Successful exploitation will allow remote attackers to poison a web-cache, perform an XSS attack and/or obtain sensitive information from requests other than their own.

Solution:**Solution type:** VendorFix

Upgrade to version 9.0.0.M13, 8.5.8, 8.0.39, 7.0.73, 6.0.48 or later.

Affected Software/OS

Apache Tomcat versions 9.0.0.M1 to 9.0.0.M11, Apache Tomcat versions 8.5.0 to 8.5.6, Apache Tomcat versions 8.0.0.RC1 to 8.0.38, Apache Tomcat versions 7.0.0 to 7.0.72, and Apache Tomcat versions 6.0.0 to 6.0.47 on Windows.

Vulnerability Insight

The code that parsed the HTTP request line permitted invalid characters. This could be exploited, in conjunction with a proxy that also permitted the invalid characters but with a different interpretation, to inject data into the HTTP response.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

... continues on next page ...

...continued from previous page...	
Details: Apache Tomcat HTTP Request Line Information Disclosure Vulnerability - Windows OID:1.3.6.1.4.1.25623.1.0.810717 Version used: 2024-02-15T05:05:40Z	
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)	
References cve: CVE-2016-6816 url: https://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.48 url: http://www.securityfocus.com/bid/94461 url: https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.73 url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.39 url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.8 url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M13 url: https://qnalist.com/questions/7885204/security-cve-2016-6816-apache-tomcat-information-disclosure cert-bund: WID-SEC-2024-0528 cert-bund: CB-K17/1746 cert-bund: CB-K17/1060 cert-bund: CB-K17/1033 cert-bund: CB-K17/0444 cert-bund: CB-K17/0397 cert-bund: CB-K17/0198 cert-bund: CB-K17/0133 cert-bund: CB-K17/0090 cert-bund: CB-K16/1976 cert-bund: CB-K16/1927 cert-bund: CB-K16/1815 dfn-cert: DFN-CERT-2017-1822 dfn-cert: DFN-CERT-2017-1095 dfn-cert: DFN-CERT-2017-1068 dfn-cert: DFN-CERT-2017-0456 dfn-cert: DFN-CERT-2017-0404 dfn-cert: DFN-CERT-2017-0203 dfn-cert: DFN-CERT-2017-0137 dfn-cert: DFN-CERT-2017-0095 dfn-cert: DFN-CERT-2016-2090 dfn-cert: DFN-CERT-2016-2035 dfn-cert: DFN-CERT-2016-1922	

High (CVSS: 7.0) NVT: Apache Tomcat RCE Vulnerability (May 2020) - Windows
Product detection result cpe:/a:apache:tomcat:7.0.61 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to a remote code execution vulnerability.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.104 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 7.0.104, 8.5.55, 9.0.35, 10.0.0-M5 or later.
Affected Software/OS Apache Tomcat 7.0.0 to 7.0.103, 8.5.0 to 8.5.54, 9.0.0.M1 to 9.0.34 and 10.0.0-M1 to 10.0.0-M4.
Vulnerability Insight If: - an attacker is able to control the contents and name of a file on the server and - the server is configured to use the PersistenceManager with a FileStore and - the PersistenceManager is configured with sessionAttributeValueClassNameFilter='null' (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized and - the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions must be true for the attack to succeed.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat RCE Vulnerability (May 2020) - Windows OID:1.3.6.1.4.1.25623.1.0.143964 Version used: 2024-02-08T05:05:59Z
... continues on next page ...

...continued from previous page ...

Product Detection Result

Product: cpe:/a:apache:tomcat:7.0.61

Method: Apache Tomcat Detection Consolidation

OID: 1.3.6.1.4.1.25623.1.0.107652)

References

cve: CVE-2020-9484

url: <https://lists.apache.org/thread.html/r77eae567ed829da9012cadb29af17f2df8fa2?3bf66faf88229857bb1%40%3Cannounce.tomcat.apache.org%3E>

cert-bund: WID-SEC-2022-1870

cert-bund: WID-SEC-2022-0607

cert-bund: WID-SEC-2022-0432

cert-bund: WID-SEC-2022-0302

cert-bund: CB-K21/1094

cert-bund: CB-K21/0069

dfn-cert: DFN-CERT-2022-1530

dfn-cert: DFN-CERT-2022-0733

dfn-cert: DFN-CERT-2021-1736

dfn-cert: DFN-CERT-2020-2286

dfn-cert: DFN-CERT-2020-1706

dfn-cert: DFN-CERT-2020-1635

dfn-cert: DFN-CERT-2020-1575

dfn-cert: DFN-CERT-2020-1490

dfn-cert: DFN-CERT-2020-1289

dfn-cert: DFN-CERT-2020-1134

dfn-cert: DFN-CERT-2020-1129

dfn-cert: DFN-CERT-2020-1094

dfn-cert: DFN-CERT-2020-1086

High (CVSS: 7.0)

NVT: Apache Tomcat RCE Vulnerability (Mar 2021) - Windows

Product detection result

cpe:/a:apache:tomcat:7.0.61

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.107652)

Summary

Apache Tomcat is prone to a remote code execution (RCE) vulnerability due to an incomplete fix.

...continues on next page ...

...continued from previous page ...
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.108 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 7.0.108, 8.5.63, 9.0.43, 10.0.2 or later.
Affected Software/OS Apache Tomcat 7.0.x - 7.0.107, 8.5.x - 8.5.61, 9.0.0.M1 - 9.0.41 and 10.0.x prior to 10.0.1.
Vulnerability Insight The fix for CVE-2020-9484 was incomplete. When using a highly unlikely configuration edge case, the Tomcat instance is still vulnerable to CVE-2020-9484. Note that both the previously published prerequisites for CVE-2020-9484 also apply to this issue.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat RCE Vulnerability (Mar 2021) - Windows OID:1.3.6.1.4.1.25623.1.0.145478 Version used: 2024-02-22T05:06:55Z
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2021-25329 url: https://lists.apache.org/thread.html/rfe62fbf9d4c314f166fe8c668e50e5d9dd882↪a99447f26f0367474bf6%3Cannounce.tomcat.apache.org%3E url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.0.2 url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.43 url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.63 url: https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.108 cert-bund: WID-SEC-2022-1099 cert-bund: WID-SEC-2022-0607 cert-bund: CB-K21/0222 dfn-cert: DFN-CERT-2022-1530 dfn-cert: DFN-CERT-2022-0733 dfn-cert: DFN-CERT-2021-1904
... continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2021-1403
dfn-cert: DFN-CERT-2021-0903
dfn-cert: DFN-CERT-2021-0835
dfn-cert: DFN-CERT-2021-0807
dfn-cert: DFN-CERT-2021-0714
dfn-cert: DFN-CERT-2021-0544
dfn-cert: DFN-CERT-2021-0445
```

High (CVSS: 7.0)

NVT: Apache Tomcat Privilege Escalation Vulnerability (Dec 2019) - Windows

Product detection result

cpe:/a:apache:tomcat:7.0.61

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)**Summary**

Apache Tomcat is prone to a privilege escalation vulnerability.

Quality of Detection: 80**Vulnerability Detection Result**

Installed version: 7.0.61

Fixed version: 7.0.99

Installation

path / port: 80/tcp

Solution:**Solution type:** VendorFix

Update to version 7.0.99, 8.5.49, 9.0.29 or later. As a mitigation disable Tomcat's JmxRemoteLifecycleListener and use the built-in remote JMX facilities provided by the JVM.

Affected Software/OS

Apache Tomcat 7.0.0 to 7.0.97, 8.5.0 to 8.5.47 and 9.0.0.M1 to 9.0.28.

Vulnerability Insight

When Tomcat is configured with the JMX Remote Lifecycle Listener, a local attacker without access to the Tomcat process or configuration files is able to manipulate the RMI registry to perform a man-in-the-middle attack to capture user names and passwords used to access the JMX interface. The attacker can then use these credentials to access the JMX interface and gain complete control over the Tomcat instance.

Vulnerability Detection Method

... continues on next page ...

...continued from previous page ...
Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Privilege Escalation Vulnerability (Dec 2019) - Windows OID:1.3.6.1.4.1.25623.1.0.143312 Version used: 2024-02-08T05:05:59Z
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2019-12418 url: https://lists.apache.org/thread.html/43530b91506e2e0c11cfbe691173f5df8c48f5%3C1b98262426d7493b67%40%3Cannounce.tomcat.apache.org%3E cert-bund: WID-SEC-2024-0528 cert-bund: WID-SEC-2023-1229 cert-bund: CB-K19/1102 dfn-cert: DFN-CERT-2020-1129 dfn-cert: DFN-CERT-2020-1094 dfn-cert: DFN-CERT-2020-0821 dfn-cert: DFN-CERT-2020-0604 dfn-cert: DFN-CERT-2020-0557 dfn-cert: DFN-CERT-2020-0501 dfn-cert: DFN-CERT-2020-0345 dfn-cert: DFN-CERT-2020-0027 dfn-cert: DFN-CERT-2019-2710 dfn-cert: DFN-CERT-2019-2673

[\[return to 192.168.0.200 \]](#)

2.1.2 Medium 3389/tcp

Medium (CVSS: 5.9) NVT: SSL/TLS: Report Weak Cipher Suites
Summary This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.
Quality of Detection: 98
... continues on next page ...

...continued from previous page...

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)
- 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: 2023-11-02T05:05:26Z

References

cve: CVE-2013-2566

cve: CVE-2015-2808

cve: CVE-2015-4000

url: https://www.bsi.bund.de/SharedDocs/Warntmeldungen/DE/CB/warntmeldung_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

...continues on next page ...

...continued from previous page ...

cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168

...continues on next page ...

...continued from previous page ...

```

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

```

Medium (CVSS: 4.3)

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

Summary

... continues on next page ...

...continued from previous page ...
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection: 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: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
Vulnerability Detection Method Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2023-10-20T16:09:12Z
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
... 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-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

... continues on next page ...

...continued from previous page ...

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
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743

...continues on next page ...

...continued from previous page ...

```
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
```

[\[return to 192.168.0.200 \]](#)**2.1.3 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: 80**Vulnerability Detection Result**

Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 11731/tcp

UUID: d107c6e0-fc35-49ba-ba03-3e192de6797d, version 1

Endpoint: ncacn_ip_tcp:192.168.0.200[11731]

Annotation: Veeam Deployer

UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1

Endpoint: ncacn_ip_tcp:192.168.0.200[11731]

Annotation: Veeam RPC Invoker

Port: 49664/tcp

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

Endpoint: ncacn_ip_tcp:192.168.0.200[49664]

Port: 49665/tcp

UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1

Endpoint: ncacn_ip_tcp:192.168.0.200[49665]

Annotation: DHCP Client LRPC Endpoint

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

Endpoint: ncacn_ip_tcp:192.168.0.200[49665]

Annotation: Event log TCPIP

Port: 49668/tcp

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

Endpoint: ncacn_ip_tcp:192.168.0.200[49668]

...continues on next page ...

...continued from previous page...

```

Annotation: RemoteAccessCheck
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
Endpoint: ncacn_ip_tcp:192.168.0.200[49668]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : SAM access
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
Endpoint: ncacn_ip_tcp:192.168.0.200[49668]
Annotation: Ngc Pop Key Service
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
Endpoint: ncacn_ip_tcp:192.168.0.200[49668]
Annotation: Ngc Pop Key Service
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
Endpoint: ncacn_ip_tcp:192.168.0.200[49668]
Annotation: KeyIso
Port: 49669/tcp
UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1
Endpoint: ncacn_ip_tcp:192.168.0.200[49669]
Annotation: UserMgrCli
UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1
Endpoint: ncacn_ip_tcp:192.168.0.200[49669]
Annotation: AppInfo
UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
Endpoint: ncacn_ip_tcp:192.168.0.200[49669]
UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
Endpoint: ncacn_ip_tcp:192.168.0.200[49669]
Annotation: Proxy Manager provider server endpoint
UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
Endpoint: ncacn_ip_tcp:192.168.0.200[49669]
UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
Endpoint: ncacn_ip_tcp:192.168.0.200[49669]
Annotation: IP Transition Configuration endpoint
UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1
Endpoint: ncacn_ip_tcp:192.168.0.200[49669]
Annotation: AppInfo
UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1
Endpoint: ncacn_ip_tcp:192.168.0.200[49669]
Annotation: AppInfo
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
Endpoint: ncacn_ip_tcp:192.168.0.200[49669]
UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
Endpoint: ncacn_ip_tcp:192.168.0.200[49669]
Annotation: IKE/Authip API
UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1
Endpoint: ncacn_ip_tcp:192.168.0.200[49669]
Annotation: UserMgrCli
UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1

```

...continues on next page ...

...continued from previous page...	
Endpoint: ncacn_ip_tcp:192.168.0.200[49669]	
Annotation: Proxy Manager client server endpoint	
UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.200[49669]	
Annotation: Adh APIs	
UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.200[49669]	
UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.200[49669]	
Annotation: AppInfo	
UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.200[49669]	
Annotation: AppInfo	
Port: 49692/tcp	
UUID: 0b6edbfba-4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.200[49692]	
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.200[49692]	
Named pipe : spoolss	
Win32 service or process : spoolsv.exe	
Description : Spooler service	
UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.200[49692]	
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.200[49692]	
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.200[49692]	
Port: 49707/tcp	
UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.200[49707]	
Annotation: Remote Fw APIs	
Port: 58731/tcp	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.200[58731]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.200[58731]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.200[58731]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.200[58731]	
Annotation: KeyIso	
Port: 58732/tcp	
...continues on next page...	

...continued from previous page...	
UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:192.168.0.200[58732]	
Port: 6160/tcp UUID: d1c2c6e0-fc35-49ba-ba03-3e192de6797d, version 1 Endpoint: ncacn_ip_tcp:192.168.0.200[6160] Annotation: Veeam Deployer UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1 Endpoint: ncacn_ip_tcp:192.168.0.200[6160] Annotation: Veeam RPC Invoker	
Port: 6162/tcp UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1 Endpoint: ncacn_ip_tcp:192.168.0.200[6162] Annotation: Veeam Invoker	
Port: 6190/tcp UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1 Endpoint: ncacn_ip_tcp:192.168.0.200[6190] Annotation: Veeam Invoker	
Port: 6210/tcp UUID: 844d6366-6a97-4eb5-8345-b88e8276c20d, version 1 Endpoint: ncacn_ip_tcp:192.168.0.200[6210] Annotation: Veeam HV Integration UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1 Endpoint: ncacn_ip_tcp:192.168.0.200[6210] Annotation: Veeam Invoker	
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.	
Impact An attacker may use this fact to gain more knowledge about the remote host.	
Solution: Solution type: Mitigation Filter incoming traffic to this ports.	
Vulnerability Detection Method Details: DCE/RPC and MSRPC Services Enumeration Reporting OID:1.3.6.1.4.1.25623.1.0.10736 Version used: 2022-06-03T10:17:07Z	

[\[return to 192.168.0.200 \]](#)

2.1.4 Medium 80/tcp

Medium (CVSS: 6.5)
NVT: Apache Tomcat Security Constraint Incorrect Handling Access Bypass Vulnerabilities - Windows
Product detection result cpe:/a:apache:tomcat:7.0.61 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to multiple access bypass vulnerabilities.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.85 Installation path / port: 80/tcp
Impact Successfully exploiting these issues will allow remote attackers to bypass security constraints to access ostensibly restricted resources on the target system.
Solution: Solution type: VendorFix Upgrade to Apache Tomcat version 9.0.5, 8.5.28, 8.0.50, 7.0.85 or later.
Affected Software/OS Apache Tomcat versions 9.0.0.M1 to 9.0.4 Apache Tomcat versions 8.5.0 to 8.5.27 Apache Tomcat versions 8.0.0.RC1 to 8.0.49 Apache Tomcat versions 7.0.0 to 7.0.84 on Windows.
Vulnerability Insight Multiple flaws are due to: - The system does not properly enforce security constraints that defined by annotations of Servlets in certain cases, depending on the order that Servlets are loaded. - The URL pattern of " (the empty string) which exactly maps to the context root was not correctly handled when used as part of a security constraint definition.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Security Constraint Incorrect Handling Access Bypass Vulnerabilit.
... continues on next page ...

...continued from previous page ...

↔..

OID:1.3.6.1.4.1.25623.1.0.812784

Version used: 2024-02-15T05:05:40Z

Product Detection Result

Product: cpe:/a:apache:tomcat:7.0.61

Method: Apache Tomcat Detection Consolidation

OID: 1.3.6.1.4.1.25623.1.0.107652)

References

cve: CVE-2018-1305

cve: CVE-2018-1304

url: <http://tomcat.apache.org/security-9.html>url: <http://www.securityfocus.com/bid/103144>url: <http://www.securityfocus.com/bid/103170>url: <http://tomcat.apache.org/security-8.html>url: <http://tomcat.apache.org/security-7.html>url: <https://lists.apache.org/thread.html/b1d7e2425d6fd2cebed40d318f9365b4454607>

↔7e10949b01b1f8a0fb0%3Cannounce.tomcat.apache.org%3E

cert-bund: WID-SEC-2024-0528

cert-bund: CB-K19/1121

cert-bund: CB-K19/0321

cert-bund: CB-K18/1007

cert-bund: CB-K18/1006

cert-bund: CB-K18/1005

cert-bund: CB-K18/0790

cert-bund: CB-K18/0420

cert-bund: CB-K18/0349

dfn-cert: DFN-CERT-2019-1627

dfn-cert: DFN-CERT-2019-0772

dfn-cert: DFN-CERT-2018-2165

dfn-cert: DFN-CERT-2018-2142

dfn-cert: DFN-CERT-2018-2125

dfn-cert: DFN-CERT-2018-2103

dfn-cert: DFN-CERT-2018-1753

dfn-cert: DFN-CERT-2018-1407

dfn-cert: DFN-CERT-2018-1274

dfn-cert: DFN-CERT-2018-1253

dfn-cert: DFN-CERT-2018-1038

dfn-cert: DFN-CERT-2018-0922

dfn-cert: DFN-CERT-2018-0733

dfn-cert: DFN-CERT-2018-0455

dfn-cert: DFN-CERT-2018-0378

Medium (CVSS: 6.5)
NVT: Apache Tomcat JNDI Realm Authentication Weakness Vulnerability (Jul 2021) - Windows
Product detection result cpe:/a:apache:tomcat:7.0.61 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to an authentication weakness vulnerability in the JNDI Realm.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.109 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 7.0.109, 8.5.66, 9.0.46, 10.0.6 or later.
Affected Software/OS Apache Tomcat 7.0.x through 7.0.108, 8.5.x through 8.5.65, 9.0.0.M1 through 9.0.45 and 10.0.0-M1 through 10.0.5.
Vulnerability Insight Queries made by the JNDI Realm do not always correctly escape parameters. Parameter values could be sourced from user provided data (eg user names) as well as configuration data provided by an administrator. In limited circumstances it is possible for users to authenticate using variations of their user name and/or to bypass some of the protection provided by the LockOut Realm.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat JNDI Realm Authentication Weakness Vulnerability (Jul 2021) - Win. ↪.. OID:1.3.6.1.4.1.25623.1.0.146265 Version used: 2021-08-24T06:00:58Z
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2021-30640 url: https://lists.apache.org/thread.html/r59f9ef03929d32120f91f4ea7e6e79edd5688 ↪d75d0a9b65fd26d1fe8%40%3Cannounce.tomcat.apache.org%3E url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.0.6 url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.46 url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.66 url: https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.109 cert-bund: WID-SEC-2024-0528 cert-bund: WID-SEC-2022-1116 cert-bund: WID-SEC-2022-0623 cert-bund: WID-SEC-2022-0615 cert-bund: WID-SEC-2022-0607 cert-bund: CB-K21/0733 dfn-cert: DFN-CERT-2022-1530 dfn-cert: DFN-CERT-2022-0826 dfn-cert: DFN-CERT-2022-0733 dfn-cert: DFN-CERT-2021-2496 dfn-cert: DFN-CERT-2021-2438 dfn-cert: DFN-CERT-2021-2297 dfn-cert: DFN-CERT-2021-2169 dfn-cert: DFN-CERT-2021-1728 dfn-cert: DFN-CERT-2021-1668 dfn-cert: DFN-CERT-2021-1472

Medium (CVSS: 6.3)

NVT: Apache Tomcat Security Manager Bypass Vulnerability (Feb 2016) - Windows

Product detection result

cpe:/a:apache:tomcat:7.0.61

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary

Apache Tomcat is prone to Security Manager Bypass Vulnerability.

Quality of Detection: 80

Vulnerability Detection Result

Installed version: 7.0.61

Fixed version: 7.0.68

... continues on next page ...

...continued from previous page ...	
Installation	
path / port:	80/tcp
Impact	Successful exploitation will allow remote authenticated users to bypass intended SecurityManager restrictions and read or write to arbitrary application data, or cause a denial of service.
Solution:	
Solution type:	VendorFix
	Upgrade to version 7.0.68 or 8.0.32 or 9.0.0.M3 or later.
Affected Software/OS	Apache Tomcat 7.0.0 before 7.0.68, 8.0.0.RC1 before 8.0.31, and 9.0.0.M1 before 9.0.0.M2 on Windows.
Vulnerability Insight	The flaw is due to an improper validation of 'ResourceLinkFactory.setGlobalContext()' method and is accessible by web applications running under a security manager without any checks.
Vulnerability Detection Method	Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Security Manager Bypass Vulnerability (Feb 2016) - Windows OID:1.3.6.1.4.1.25623.1.0.807406 Version used: 2024-02-08T05:05:59Z
Product Detection Result	Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References	cve: CVE-2016-0763 url: http://tomcat.apache.org/security-9.html url: http://www.securityfocus.com/bid/83326 url: http://tomcat.apache.org/security-8.html url: http://tomcat.apache.org/security-7.html cert-bund: CB-K17/1750 cert-bund: CB-K17/0661 cert-bund: CB-K17/0098 cert-bund: CB-K16/1799 cert-bund: CB-K16/1758 cert-bund: CB-K16/1622 cert-bund: CB-K16/0993 cert-bund: CB-K16/0789 cert-bund: CB-K16/0758
... continues on next page ...	

...continued from previous page ...

cert-bund: CB-K16/0476
 cert-bund: CB-K16/0292
 dfn-cert: DFN-CERT-2017-1821
 dfn-cert: DFN-CERT-2017-0677
 dfn-cert: DFN-CERT-2017-0090
 dfn-cert: DFN-CERT-2016-1905
 dfn-cert: DFN-CERT-2016-1823
 dfn-cert: DFN-CERT-2016-1715
 dfn-cert: DFN-CERT-2016-1059
 dfn-cert: DFN-CERT-2016-0842
 dfn-cert: DFN-CERT-2016-0807
 dfn-cert: DFN-CERT-2016-0518
 dfn-cert: DFN-CERT-2016-0314

Medium (CVSS: 6.1)

NVT: Apache Tomcat XSS Vulnerability (May 2019) - Windows

Product detection result

cpe:/a:apache:tomcat:7.0.61

Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
 ↪7652)**Summary**

Apache Tomcat is prone to a cross-site scripting vulnerability.

Quality of Detection: 80**Vulnerability Detection Result**

Installed version: 7.0.61

Fixed version: 7.0.94

Installation

path / port: 80/tcp

Solution:**Solution type:** VendorFix

Update to version 7.0.94, 8.5.40, 9.0.18 or later.

Affected Software/OS

Apache Tomcat versions 7.0.0 to 7.0.93, 8.5.0 to 8.5.39 and 9.0.0.M1 to 9.0.17.

Vulnerability Insight

... continues on next page ...

...continued from previous page ...
<p>The SSI printenv command in Apache Tomcat echoes user provided data without escaping and is, therefore, vulnerable to XSS. SSI is disabled by default. The printenv command is intended for debugging and is unlikely to be present in a production website.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat XSS Vulnerability (May 2019) - Windows OID:1.3.6.1.4.1.25623.1.0.142480 Version used: 2024-02-08T05:05:59Z</p>
<p>Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)</p>
<p>References cve: CVE-2019-0221 url: https://seclists.org/fulldisclosure/2019/May/50 url: https://lists.apache.org/thread.html/6e6e9eacf7b28fd63d249711e9d3ccd4e0a83f↪556e324aee37be5a8c0%3Cannounce.tomcat.apache.org%3E cert-bund: WID-SEC-2024-0528 cert-bund: WID-SEC-2023-1994 cert-bund: CB-K19/0434 dfn-cert: DFN-CERT-2021-0819 dfn-cert: DFN-CERT-2020-1129 dfn-cert: DFN-CERT-2020-1094 dfn-cert: DFN-CERT-2020-0557 dfn-cert: DFN-CERT-2019-2710 dfn-cert: DFN-CERT-2019-2457 dfn-cert: DFN-CERT-2019-1895 dfn-cert: DFN-CERT-2019-1704 dfn-cert: DFN-CERT-2019-1472 dfn-cert: DFN-CERT-2019-1231 dfn-cert: DFN-CERT-2019-1092</p>
Medium (CVSS: 5.9)
NVT: Apache Tomcat Information Disclosure Vulnerability (Jan 2021) - Windows
<p>Product detection result cpe:/a:apache:tomcat:7.0.61 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10↪7652)</p>
... continues on next page ...

...continued from previous page ...
Summary Apache Tomcat is prone to an information disclosure vulnerability.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.107 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 7.0.107, 8.5.60, 9.0.40, 10.0.0-M10 or later.
Affected Software/OS Apache Tomcat 7.0.0 to 7.0.106, 8.5.0 to 8.5.59, 9.0.0-M1 to 9.0.39 and 10.0.0-M1 to 10.0.0-M9.
Vulnerability Insight When serving resources from a network location using the NTFS file system it was possible to bypass security constraints and/or view the source code for JSPs in some configurations. The root cause was the unexpected behaviour of the JRE API File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API (FindFirstFileW) in some circumstances.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Information Disclosure Vulnerability (Jan 2021) - Windows OID:1.3.6.1.4.1.25623.1.0.117158 Version used: 2024-02-08T05:05:59Z
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2021-24122 url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.0.0-M1 ↪0 url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.40 url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.60 url: https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.107 url: https://lists.apache.org/thread.html/rce5ac9a40173651d540babce59f6f3825f12c ↪6d4e886ba00823b11e5%40%3Cannounce.tomcat.apache.org%3E
... continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2023-2465
cert-bund: WID-SEC-2022-0607
cert-bund: CB-K21/0049
dfn-cert: DFN-CERT-2022-1530
dfn-cert: DFN-CERT-2021-1904
dfn-cert: DFN-CERT-2021-0835
dfn-cert: DFN-CERT-2021-0714
dfn-cert: DFN-CERT-2021-0544
dfn-cert: DFN-CERT-2021-0338
dfn-cert: DFN-CERT-2020-2646

Medium (CVSS: 5.3)
NVT: Apache Tomcat Directory Disclosure Vulnerability (Feb 2016) - Windows
Product detection result cpe:/a:apache:tomcat:7.0.61 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to Directory Disclosure Vulnerability.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.67 Installation path / port: 80/tcp
Impact Successful exploitation allows remote attackers to determine the existence of a directory.
Solution: Solution type: VendorFix Upgrade to version 6.0.45 or 7.0.67 or 8.0.30 or 9.0.0.M3 later.
Affected Software/OS Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.67, 8.0.0.RC1 before 8.0.30, and 9.0.0.M1 on Windows.
Vulnerability Insight ... continues on next page ...

...continued from previous page...
The flaw is due to an improper accessing a directory protected by a security constraint with a URL that did not end in a slash.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Directory Disclosure Vulnerability (Feb 2016) - Windows OID:1.3.6.1.4.1.25623.1.0.807407 Version used: 2024-02-08T05:05:59Z
Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)
References cve: CVE-2015-5345 url: http://tomcat.apache.org/security-9.html url: http://www.securityfocus.com/bid/83328 url: http://tomcat.apache.org/security-8.html url: http://tomcat.apache.org/security-7.html url: http://tomcat.apache.org/security-6.html url: https://bz.apache.org/bugzilla/show_bug.cgi?id=58765 cert-bund: CB-K16/1758 cert-bund: CB-K16/1630 cert-bund: CB-K16/1568 cert-bund: CB-K16/0993 cert-bund: CB-K16/0789 cert-bund: CB-K16/0758 cert-bund: CB-K16/0496 cert-bund: CB-K16/0476 cert-bund: CB-K16/0292 dfn-cert: DFN-CERT-2016-1823 dfn-cert: DFN-CERT-2016-1726 dfn-cert: DFN-CERT-2016-1661 dfn-cert: DFN-CERT-2016-1059 dfn-cert: DFN-CERT-2016-0842 dfn-cert: DFN-CERT-2016-0807 dfn-cert: DFN-CERT-2016-0537 dfn-cert: DFN-CERT-2016-0518 dfn-cert: DFN-CERT-2016-0314

Medium (CVSS: 4.3)
NVT: Apache Tomcat Open Redirect Vulnerability - Windows
<p>Product detection result</p> <p>cpe:/a:apache:tomcat:7.0.61</p> <p>Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)</p>
<p>Summary</p> <p>When the default servlet in Apache Tomcat returned a redirect to a directory (e.g. redirecting to '/foo/' when the user requested '/foo') a specially crafted URL could be used to cause the redirect to be generated to any URI of the attackers choice.</p>
<p>Quality of Detection: 80</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 7.0.61</p> <p>Fixed version: 7.0.91</p> <p>Installation path / port: 80/tcp</p>
<p>Solution:</p> <p>Solution type: VendorFix</p> <p>Update to version 7.0.91, 8.5.34, 9.0.12 or later.</p>
<p>Affected Software/OS</p> <p>Apache Tomcat 9.0.0.M1-9.0.11, 8.5.0-8.5.33, 7.0.23-7.0.90 and probably 8.0.x.</p>
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Apache Tomcat Open Redirect Vulnerability - Windows</p> <p>OID:1.3.6.1.4.1.25623.1.0.141569</p> <p>Version used: 2024-02-15T05:05:40Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:apache:tomcat:7.0.61</p> <p>Method: Apache Tomcat Detection Consolidation</p> <p>OID: 1.3.6.1.4.1.25623.1.0.107652)</p>
<p>References</p> <p>cve: CVE-2018-11784</p> <p>url: http://tomcat.apache.org/security-9.html</p> <p>url: http://tomcat.apache.org/security-8.html</p> <p>... continues on next page ...</p>

...continued from previous page ...

```

url: http://tomcat.apache.org/security-7.html
cert-bund: WID-SEC-2024-0528
cert-bund: WID-SEC-2023-0531
cert-bund: WID-SEC-2023-0460
cert-bund: CB-K19/1121
cert-bund: CB-K19/0907
cert-bund: CB-K19/0616
cert-bund: CB-K19/0320
cert-bund: CB-K19/0050
cert-bund: CB-K18/0963
dfn-cert: DFN-CERT-2019-2710
dfn-cert: DFN-CERT-2019-2159
dfn-cert: DFN-CERT-2019-1562
dfn-cert: DFN-CERT-2019-1237
dfn-cert: DFN-CERT-2019-0771
dfn-cert: DFN-CERT-2019-0147
dfn-cert: DFN-CERT-2019-0104
dfn-cert: DFN-CERT-2018-2435
dfn-cert: DFN-CERT-2018-2165
dfn-cert: DFN-CERT-2018-2142
dfn-cert: DFN-CERT-2018-2000

```

Medium (CVSS: 4.3)

NVT: Apache Tomcat Information Disclosure Vulnerability (Mar 2023) - Windows

Product detection result

```

cpe:/a:apache:tomcat:7.0.61
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

```

Summary

Apache Tomcat is prone to an information disclosure vulnerability.

Quality of Detection: 80**Vulnerability Detection Result**

```

Installed version: 7.0.61
Fixed version:      8.5.86
Installation
path / port:        80/tcp

```

Solution:**Solution type:** VendorFix

Update to version 8.5.86, 9.0.72, 10.1.6, 11.0.0-M3 or later.

... continues on next page ...

...continued from previous page ...
<p>Affected Software/OS Apache Tomcat versions through 8.5.85, 9.0.0-M1 through 9.0.71, 10.x through 10.1.5 and 11.0.0-M1 through 11.0.0-M2.</p>
<p>Vulnerability Insight When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Tomcat did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Information Disclosure Vulnerability (Mar 2023) - Windows OID:1.3.6.1.4.1.25623.1.0.104654 Version used: 2023-10-12T05:05:32Z</p>
<p>Product Detection Result Product: cpe:/a:apache:tomcat:7.0.61 Method: Apache Tomcat Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.107652)</p>
<p>References cve: CVE-2023-28708 url: https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67 url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M3 url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.6 url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.72 url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.86 cert-bund: WID-SEC-2024-0528 cert-bund: WID-SEC-2023-2674 cert-bund: WID-SEC-2023-1812 cert-bund: WID-SEC-2023-1808 cert-bund: WID-SEC-2023-1784 cert-bund: WID-SEC-2023-1783 cert-bund: WID-SEC-2023-1782 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-1021 cert-bund: WID-SEC-2023-1017 cert-bund: WID-SEC-2023-0717 dfn-cert: DFN-CERT-2023-2778 dfn-cert: DFN-CERT-2023-2545 dfn-cert: DFN-CERT-2023-2054 dfn-cert: DFN-CERT-2023-0772 dfn-cert: DFN-CERT-2023-0763</p>
...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2023-0640

Medium (CVSS: 4.3)
NVT: Apache Tomcat Limited Directory Traversal Vulnerability (Feb 2016) - Windows
Product detection result cpe:/a:apache:tomcat:7.0.61 Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10 ↪7652)
Summary Apache Tomcat is prone to a limited directory traversal vulnerability.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 7.0.61 Fixed version: 7.0.65 Installation path / port: 80/tcp
Impact Successful exploitation will allow remote authenticated users to bypass intended SecurityManager restrictions and list a parent directory.
Solution: Solution type: VendorFix Upgrade to version 6.0.45 or 7.0.65 or 8.0.27 or later.
Affected Software/OS Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.65, and 8.0.0.RC1 before 8.0.27 on Windows.
Vulnerability Insight The flaw is due to an improper validation of path while accessing resources via the ServletContext methods getResource(), getResourceAsStream() and getResourcePaths() the paths should be limited to the current web application.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache Tomcat Limited Directory Traversal Vulnerability (Feb 2016) - Windows OID:1.3.6.1.4.1.25623.1.0.807404 Version used: 2024-02-08T05:05:59Z
... continues on next page ...

...continued from previous page ...

Product Detection Result

Product: cpe:/a:apache:tomcat:7.0.61

Method: Apache Tomcat Detection Consolidation

OID: 1.3.6.1.4.1.25623.1.0.107652)

References

cve: CVE-2015-5174

url: <http://tomcat.apache.org/security-9.html>url: <http://www.securityfocus.com/bid/83329>url: <http://tomcat.apache.org/security-8.html>url: <http://tomcat.apache.org/security-7.html>url: <http://tomcat.apache.org/security-6.html>

cert-bund: CB-K18/0066

cert-bund: CB-K16/1758

cert-bund: CB-K16/1630

cert-bund: CB-K16/1568

cert-bund: CB-K16/1089

cert-bund: CB-K16/0993

cert-bund: CB-K16/0789

cert-bund: CB-K16/0587

cert-bund: CB-K16/0496

cert-bund: CB-K16/0476

cert-bund: CB-K16/0292

cert-bund: CB-K15/1841

dfn-cert: DFN-CERT-2018-0077

dfn-cert: DFN-CERT-2016-1823

dfn-cert: DFN-CERT-2016-1726

dfn-cert: DFN-CERT-2016-1661

dfn-cert: DFN-CERT-2016-1161

dfn-cert: DFN-CERT-2016-1059

dfn-cert: DFN-CERT-2016-0842

dfn-cert: DFN-CERT-2016-0635

dfn-cert: DFN-CERT-2016-0537

dfn-cert: DFN-CERT-2016-0518

dfn-cert: DFN-CERT-2016-0314

dfn-cert: DFN-CERT-2015-1950

[\[return to 192.168.0.200 \]](#)**2.1.5 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: 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.200 \]](#)

2.2 192.168.0.42

Host scan start Sun May 5 04:50:39 2024 UTC

Host scan end Sun May 5 05:47:48 2024 UTC

Service (Port)	Threat Level
443/tcp	High
443/tcp	Medium
21/tcp	Medium
25/tcp	Medium
22/tcp	Low
general/icmp	Low

2.2.1 High 443/tcp

High (CVSS: 9.8)

NVT: ownCloud < 10.8 Multiple Vulnerabilities

Summary

ownCloud is prone to multiple vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result

Installed version: 10.3.0

Fixed version: 10.8

Installation

path / port: /

Solution:

Solution type: VendorFix

Update to version 10.8 or later.

Affected Software/OS

ownCloud version 10.7 and prior.

Vulnerability Insight

The following vulnerabilities exist:

- CVE-2021-35946: Federated share recipient can increase permissions
- CVE-2021-35947: Full path and username disclosure in public links
- CVE-2021-35948: Session fixation on public links
- CVE-2021-35949: Shareinfo url doesn't verify file drop permissions

Vulnerability Detection Method

... continues on next page ...

...continued from previous page ...
<p>Checks if a vulnerable version is present on the target host. Details: ownCloud < 10.8 Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.117618 Version used: 2023-12-01T16:11:30Z</p>
<p>References cve: CVE-2021-35946 cve: CVE-2021-35947 cve: CVE-2021-35948 cve: CVE-2021-35949 url: https://owncloud.com/security-advisories/cve-2021-35946/ url: https://owncloud.com/security-advisories/cve-2021-35947/ url: https://owncloud.com/security-advisories/cve-2021-35948/ url: https://owncloud.com/security-advisories/cve-2021-35949/</p>

<p>High (CVSS: 9.1) NVT: ownCloud < 10.6 Multiple Vulnerabilities</p>
<p>Summary ownCloud is prone to multiple vulnerabilities.</p>
<p>Quality of Detection: 80</p>
<p>Vulnerability Detection Result Installed version: 10.3.0 Fixed version: 10.6 Installation path / port: /</p>
<p>Solution: Solution type: VendorFix Update to version 10.6 or later.</p>
<p>Affected Software/OS ownCloud versions prior to 10.6.</p>
<p>Vulnerability Insight The following vulnerabilities exist: - Cross-Site Request Forgery in the ocs api (CVE-2020-28644) - Missing user validation is leading to information disclosure (CVE-2020-28645)</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ownCloud < 10.6 Multiple Vulnerabilities</p>
<p>... continues on next page ...</p>

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.145367 Version used: 2023-12-01T16:11:30Z
References cve: CVE-2020-28644 cve: CVE-2020-28645 url: https://owncloud.com/security-advisories/cross-site-request-forgery-in-the-ocs-api/ url: https://owncloud.com/security-advisories/missing-user-validation-leading-to-information-disclosure/

High (CVSS: 8.3) NVT: ownCloud < 10.3.2 SSRF Vulnerability
Summary ownCloud is prone to a server-side request forgery vulnerability in the 'Add to your ownCloud' functionality.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 10.3.0 Fixed version: 10.3.2 Installation path / port: /
Impact An authenticated attacker can interact with local services blindly (aka Blind SSRF) or conduct a Denial Of Service attack.
Solution: Solution type: VendorFix Update to version 10.3.2 or later.
Affected Software/OS ownCloud version 10.3.1 and prior.
Vulnerability Insight It is possible to force the ownCloud server to execute GET requests against a crafted URL on the internal or external network (Server Side Request Forgery) after receiving a public link-share URL. The criticality of this issue is lowered because the attacker can not see the result of the forged request thus there is no possibility to exfiltrate any data from an internal resource.
Vulnerability Detection Method ... continues on next page ...

...continued from previous page ...
<p>Checks if a vulnerable version is present on the target host. Details: ownCloud < 10.3.2 SSRF Vulnerability OID:1.3.6.1.4.1.25623.1.0.144860 Version used: 2023-12-01T16:11:30Z</p>
<p>References cve: CVE-2020-10252 url: https://owncloud.com/security-advisories/ssrf-in-add-to-your-owncloud-functionality/</p>

<p>High (CVSS: 7.5) NVT: ownCloud < 10.10.0 Information Disclosure Vulnerability</p>
<p>Summary ownCloud is prone to an information disclosure vulnerability.</p>
<p>Quality of Detection: 80</p>
<p>Vulnerability Detection Result Installed version: 10.3.0 Fixed version: 10.10.0 Installation path / port: /</p>
<p>Solution: Solution type: VendorFix Update to version 10.10.0 or later.</p>
<p>Affected Software/OS ownCloud prior to version 10.10.0.</p>
<p>Vulnerability Insight The settings page and some API responses of a few ownCloud apps contain plaintext credentials.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ownCloud < 10.10.0 Information Disclosure Vulnerability OID:1.3.6.1.4.1.25623.1.0.148256 Version used: 2023-12-01T16:11:30Z</p>
<p>References cve: CVE-2022-31649 url: https://owncloud.com/security-advisories/cve-2022-31649/</p>

[\[return to 192.168.0.42 \]](#)

2.2.2 Medium 443/tcp

Medium (CVSS: 6.5)
NVT: ownCloud < 10.7 Information Disclosure Vulnerability
Summary ownCloud is prone to an information disclosure vulnerability.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 10.3.0 Fixed version: 10.7 Installation path / port: /
Solution: Solution type: VendorFix Update to version 10.7 or later.
Affected Software/OS ownCloud version 10.6 and probably prior.
Vulnerability Insight The sharing dialog implements a user enumeration mitigation to prevent an authenticated user from getting a list of all accounts registered on the instance via the auto-complete dropdown. In the default configuration at least 3 characters of the name or email of the share-receiver ('Sharee') must match an existing account to trigger the autocomplete. Due to a bug in the related api endpoint the attacker can enumerate all users in a single request by entering three whitespaces. Secondary the retrieval of all users on a large instance could cause higher than average load on the instance.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ownCloud < 10.7 Information Disclosure Vulnerability OID:1.3.6.1.4.1.25623.1.0.145995 Version used: 2023-12-01T16:11:30Z
References cve: CVE-2021-29659 url: https://owncloud.com/security-advisories/cve-2021-29659/

Medium (CVSS: 6.1)
NVT: ownCloud < 10.5 XSS Vulnerability
Summary ownCloud is prone to a reflected cross-site scripting vulnerability in the forgot password functionality.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 10.3.0 Fixed version: 10.5 Installation path / port: /
Solution: Solution type: VendorFix Update to version 10.5 or later.
Affected Software/OS ownCloud versions prior to 10.5.
Vulnerability Insight The login page is not properly sanitizing exception messages from the ownCloud server.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ownCloud < 10.5 XSS Vulnerability OID:1.3.6.1.4.1.25623.1.0.145104 Version used: 2023-12-01T16:11:30Z
References cve: CVE-2020-16255 url: https://owncloud.com/security-advisories/reflected-xss-in-login-page-forgot-password-functionality/ cert-bund: WID-SEC-2023-2476

Medium (CVSS: 5.9)
NVT: ownCloud < 10.4 Access Control Vulnerability
Summary ownCloud is prone to an access control vulnerability.
...
... continues on next page ...

...continued from previous page ...
Quality of Detection: 80
Vulnerability Detection Result Installed version: 10.3.0 Fixed version: 10.4 Installation path / port: /
Impact An attacker can bypass authentication on a password-protected image by displaying its preview.
Solution: Solution type: VendorFix Update to version 10.4 or later.
Affected Software/OS ownCloud prior to version 10.4.
Vulnerability Insight It was possible to access the preview-image of a password-protected public-link. The severity of the issue is reduced to low because the attacker needs to know the public-link hash and the original filename of the image.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ownCloud < 10.4 Access Control Vulnerability OID:1.3.6.1.4.1.25623.1.0.144861 Version used: 2023-12-01T16:11:30Z
References cve: CVE-2020-10254 url: https://owncloud.com/security-advisories/public-link-password-bypass-via-image-previews/

Medium (CVSS: 5.7)
NVT: ownCloud 10.0.9 < 10.3.1 File Permission Vulnerability
Summary ownCloud is prone to a vulnerability where it is possible to access all file versions of a user.
Quality of Detection: 80
Vulnerability Detection Result Installed version: 10.3.0
...continues on next page ...

...continued from previous page...	
Fixed version:	10.3.1
Installation path / port:	/
Impact Successful exploitation allows an attacker, who has one outgoing share from a victim, to access any version of any file by sending a request for a predictable ID number.	
Solution: Solution type: VendorFix Update to version 10.3.1 or later.	
Affected Software/OS ownCloud version 10.0.9 - 10.3.0.	
Vulnerability Insight An authenticated attacker can access all versions of all files (even unshared) as soon as the owner of said files has at least one outgoing share with the attacker. To attacker needs to guess a file-id which is numeric and sequential.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ownCloud 10.0.9 < 10.3.1 File Permission Vulnerability OID:1.3.6.1.4.1.25623.1.0.144859 Version used: 2023-12-01T16:11:30Z	
References cve: CVE-2020-36252 url: https://owncloud.com/security-advisories/access-to-all-file-versions/	

Medium (CVSS: 4.3)

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

Summary

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

Quality of Detection: 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.
<p>Impact</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>Solution:</p> <p>Solution type: 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>Affected Software/OS</p> <p>All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.</p>
<p>Vulnerability Insight</p> <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: 2023-10-20T16:09:12Z</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: 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>
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-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

...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482

[\[return to 192.168.0.42 \]](#)

2.2.3 Medium 21/tcp

Medium (CVSS: 6.4)
NVT: Anonymous FTP Login Reporting
Summary Reports if the remote FTP Server allows anonymous logins.
Quality of Detection: 80
Vulnerability Detection Result It was possible to login to the remote FTP service with the following anonymous ↪account(s): anonymous:anonymous@example.com ftp:anonymous@example.com Here are the contents of the remote FTP directory listing: Account "anonymous": -rwxr-xr-x 1 ftp ftp 189 Jul 19 2019 welcome.msg Account "ftp": -rwxr-xr-x 1 ftp ftp 189 Jul 19 2019 welcome.msg
Impact Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to: - gain access to sensitive files - upload or delete files.
Solution: Solution type: Mitigation If you do not want to share files, you should disable anonymous logins.
Vulnerability Insight A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data. Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.
Vulnerability Detection Method Details: Anonymous FTP Login Reporting OID:1.3.6.1.4.1.25623.1.0.900600 Version used: 2021-10-20T09:03:29Z
... continues on next page ...

...continued from previous page ...

References

cve: CVE-1999-0497

Medium (CVSS: 4.8)

NVT: FTP Unencrypted Cleartext Login

Summary

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

Quality of Detection: 70**Vulnerability Detection Result**

The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↵. Response(s):

Non-anonymous sessions: 331 Password required for openvasvt

Anonymous sessions: 331 Anonymous login ok, send your complete email address
↵ as your password

Impact

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

Solution:

Solution type: Mitigation

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

Vulnerability Detection Method

Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.

Details: FTP Unencrypted Cleartext Login

OID:1.3.6.1.4.1.25623.1.0.108528

Version used: 2023-12-20T05:05:58Z

[\[return to 192.168.0.42 \]](#)

2.2.4 Medium 25/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
Summary The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.
Quality of Detection: 70
Vulnerability Detection Result The following indicates that the remote SSL/TLS service is affected: Protocol Version Successful re-done SSL/TLS handshakes (Renegotiation) over an ↪ existing / already established SSL/TLS connection ----- ↪----- TLSv1.0 10 TLSv1.1 10 TLSv1.2 10
Impact The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.
Solution: Solution type: VendorFix Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.
Affected Software/OS Every SSL/TLS service which does not properly restrict client-initiated renegotiation.
Vulnerability Insight The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols. Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale: > It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment. Both CVEs are still kept in this VT as a reference to the origin of this flaw.
Vulnerability Detection Method Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection. Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) OID:1.3.6.1.4.1.25623.1.0.117761
... continues on next page ...

...continued from previous page ...
Version used: 2024-02-02T05:06:11Z
References cve: CVE-2011-1473 cve: CVE-2011-5094 url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego ↔tiation-dos/ url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/ url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation url: https://www.openwall.com/lists/oss-security/2011/07/08/2 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K17/0980 cert-bund: CB-K17/0979 cert-bund: CB-K13/0915 cert-bund: CB-K13/0462 dfn-cert: DFN-CERT-2017-1013 dfn-cert: DFN-CERT-2017-1012 dfn-cert: DFN-CERT-2014-0809 dfn-cert: DFN-CERT-2013-1928 dfn-cert: DFN-CERT-2012-1112
Medium (CVSS: 5.0)
NVT: Check if Mailserver answer to VRFY and EXPN requests
Summary The Mailserver on this host answers to VRFY and/or EXPN requests.
Quality of Detection: 99
Vulnerability Detection Result 'VRFY root' produces the following answer: 252 2.0.0 root
Solution: Solution type: Workaround Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.
Vulnerability Insight VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Details: Check if Mailserver answer to VRFY and EXPN requests OID:1.3.6.1.4.1.25623.1.0.100072 Version used: 2023-10-31T05:06:37Z
References url: http://cr.yp.to/smtp/vrfy.html

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection: 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: - 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)
... continues on next page ...

...continued from previous page ...

Vulnerability Detection Method

Check the used TLS protocols of the services provided by this system.

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

OID:1.3.6.1.4.1.25623.1.0.117274

Version used: 2023-10-20T16:09:12Z

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-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

...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

```

[\[return to 192.168.0.42 \]](#)

2.2.5 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

The remote SSH server supports the following weak client-to-server MAC algorithm \hookrightarrow (s):

```

umac-64-etm@openssh.com
umac-64@openssh.com

```

The remote SSH server supports the following weak server-to-client MAC algorithm \hookrightarrow (s):

```

umac-64-etm@openssh.com
umac-64@openssh.com

```

Solution:

... continues on next page ...

...continued from previous page ...
Solution type: Mitigation Disable the reported weak MAC algorithm(s).
Vulnerability Detection Method Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: <ul style="list-style-type: none"> - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[[return to 192.168.0.42](#)]

2.2.6 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: 80
Vulnerability Detection Result The following response / ICMP packet has been received: <ul style="list-style-type: none"> - 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:
... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - 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)
<p>Vulnerability Insight</p> <p>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.</p>
<p>Vulnerability Detection Method</p> <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 OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2023-05-11T09:09:33Z</p>
<p>References</p> <p>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 dfn-cert: DFN-CERT-2014-0658</p>

[\[return to 192.168.0.42 \]](#)

2.3 192.168.0.6

Host scan start Sun May 5 03:01:04 2024 UTC
Host scan end Sun May 5 03:38:58 2024 UTC

Service (Port)	Threat Level
3389/tcp	Medium
135/tcp	Medium

2.3.1 Medium 3389/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites
<p>Summary</p> <p>This routine reports all Weak SSL/TLS cipher suites accepted by a service.</p> <p>... continues on next page ...</p>

...continued from previous page ...
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.
Quality of Detection: 98
Vulnerability Detection Result 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA '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) - 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: 2023-11-02T05:05:26Z
References cve: CVE-2013-2566 cve: CVE-2015-2808 cve: CVE-2015-4000 url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1↪465_update_6.html url: https://bettercrypto.org/ url: https://mozilla.github.io/server-side-tls/ssl-config-generator/cert-bund:CB-K21/0067
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K19/0812
 cert-bund: CB-K17/1750
 cert-bund: CB-K16/1593
 cert-bund: CB-K16/1552
 cert-bund: CB-K16/1102
 cert-bund: CB-K16/0617
 cert-bund: CB-K16/0599
 cert-bund: CB-K16/0168
 cert-bund: CB-K16/0121
 cert-bund: CB-K16/0090
 cert-bund: CB-K16/0030
 cert-bund: CB-K15/1751
 cert-bund: CB-K15/1591
 cert-bund: CB-K15/1550
 cert-bund: CB-K15/1517
 cert-bund: CB-K15/1514
 cert-bund: CB-K15/1464
 cert-bund: CB-K15/1442
 cert-bund: CB-K15/1334
 cert-bund: CB-K15/1269
 cert-bund: CB-K15/1136
 cert-bund: CB-K15/1090
 cert-bund: CB-K15/1059
 cert-bund: CB-K15/1022
 cert-bund: CB-K15/1015
 cert-bund: CB-K15/0986
 cert-bund: CB-K15/0964
 cert-bund: CB-K15/0962
 cert-bund: CB-K15/0932
 cert-bund: CB-K15/0927
 cert-bund: CB-K15/0926
 cert-bund: CB-K15/0907
 cert-bund: CB-K15/0901
 cert-bund: CB-K15/0896
 cert-bund: CB-K15/0889
 cert-bund: CB-K15/0877
 cert-bund: CB-K15/0850
 cert-bund: CB-K15/0849
 cert-bund: CB-K15/0834
 cert-bund: CB-K15/0827
 cert-bund: CB-K15/0802
 cert-bund: CB-K15/0764
 cert-bund: CB-K15/0733
 cert-bund: CB-K15/0667
 cert-bund: CB-K13/0942
 dfn-cert: DFN-CERT-2023-2939
 dfn-cert: DFN-CERT-2021-0775

... continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection: 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: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
Vulnerability Detection Method Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2023-10-20T16:09:12Z
References cve: CVE-2011-3389 cve: CVE-2015-0204 ... continues on next page ...

...continued from previous page ...

```

url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↔-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-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

```

... continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953

...continues on next page ...

...	...continued from previous page...
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

[\[return to 192.168.0.6 \]](#)

2.3.2 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting
<p>Summary</p> <p>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.</p>
<p>Quality of Detection: 80</p>
<p>Vulnerability Detection Result</p> <p>Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:</p> <p>Port: 49664/tcp</p> <p> UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1</p> <p> Endpoint: ncacn_ip_tcp:192.168.0.6[49664]</p> <p>Port: 49665/tcp</p> <p> UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1</p> <p> Endpoint: ncacn_ip_tcp:192.168.0.6[49665]</p> <p> Annotation: DHCP Client LRPC Endpoint</p> <p> UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1</p> <p> Endpoint: ncacn_ip_tcp:192.168.0.6[49665]</p> <p> Annotation: DHCPv6 Client LRPC Endpoint</p> <p> UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1</p> <p> Endpoint: ncacn_ip_tcp:192.168.0.6[49665]</p> <p> Annotation: Event log TCPIP</p> <p>Port: 49668/tcp</p> <p> UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1</p> <p>...continues on next page...</p>

...continued from previous page...	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
Annotation: UserMgrCli	
UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
Annotation: AppInfo	
UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
Annotation: Proxy Manager provider server endpoint	
UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
Annotation: IP Transition Configuration endpoint	
UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
Annotation: AppInfo	
UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
Annotation: AppInfo	
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
Annotation: UserMgrCli	
UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
Annotation: Proxy Manager client server endpoint	
UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
Annotation: Adh APIs	
UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
Annotation: Impl friendly name	
UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
Annotation: AppInfo	
UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49668]	
Annotation: AppInfo	
Port: 49670/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
...continues on next page...	

...continued from previous page...	
Endpoint: ncacn_ip_tcp:192.168.0.6[49670]	
Annotation: RemoteAccessCheck	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49670]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49670]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49670]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.6[49670]	
Annotation: KeyIso	
Port: 49671/tcp	
UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49671]	
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49671]	
Named pipe : spoolss	
Win32 service or process : spoolsv.exe	
Description : Spooler service	
UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49671]	
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49671]	
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49671]	
Port: 49713/tcp	
UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.6[49713]	
Port: 49722/tcp	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.6[49722]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
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.	
Impact	
An attacker may use this fact to gain more knowledge about the remote host.	
Solution:	
...continues on next page...	

...continued from previous page ...

Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method

Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: 2022-06-03T10:17:07Z

[\[return to 192.168.0.6 \]](#)

2.4 192.168.0.241

Host scan start Sun May 5 03:01:04 2024 UTC

Host scan end Sun May 5 03:37:58 2024 UTC

Service (Port)	Threat Level
135/tcp	Medium
3389/tcp	Medium
general/icmp	Low

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

Endpoint: ncacn_ip_tcp:192.168.0.241[49664]

Port: 49665/tcp

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

Endpoint: ncacn_ip_tcp:192.168.0.241[49665]

Annotation: Event log TCPIP

... continues on next page ...

...continued from previous page...	
Port: 49666/tcp	
UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
Annotation: UserMgrCli	
UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
Annotation: AppInfo	
UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
Annotation: Proxy Manager provider server endpoint	
UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
Annotation: IP Transition Configuration endpoint	
UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
Annotation: AppInfo	
UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
Annotation: AppInfo	
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
Annotation: IKE/Authip API	
UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
Annotation: UserMgrCli	
UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
Annotation: Proxy Manager client server endpoint	
UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
Annotation: Adh APIs	
UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
Annotation: Impl friendly name	
UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
Annotation: AppInfo	
UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49666]	
...continues on next page...	

...continued from previous page...	
Annotation: AppInfo	
Port: 49667/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_ip_tcp:192.168.0.241[49667]	
Annotation: RemoteAccessCheck	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49667]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49667]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49667]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.241[49667]	
Annotation: KeyIso	
Port: 49689/tcp	
UUID: 0b6edbf8-4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49689]	
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49689]	
Named pipe : spoolss	
Win32 service or process : spoolsv.exe	
Description : Spooler service	
UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49689]	
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49689]	
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49689]	
Port: 49705/tcp	
UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.241[49705]	
Port: 49708/tcp	
UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[49708]	
Annotation: Remote Fw APIs	
Port: 5040/tcp	
UUID: 1a927394-352e-4553-ae3f-7cf4aafca620, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[5040]	
Port: 64381/tcp	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.241[64381]	
Named pipe : lsass	
...continues on next page...	

<p>...continued from previous page ...</p> <p>Win32 service or process : lsass.exe Description : SAM access UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1 Endpoint: ncacn_ip_tcp:192.168.0.241[64381] Annotation: Ngc Pop Key Service UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:192.168.0.241[64381] Annotation: Ngc Pop Key Service UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:192.168.0.241[64381] Annotation: KeyIso</p> <p>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.</p>
<p>Impact An attacker may use this fact to gain more knowledge about the remote host.</p>
<p>Solution: Solution type: Mitigation Filter incoming traffic to this ports.</p>
<p>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</p>

[\[return to 192.168.0.241 \]](#)

2.4.2 Medium 3389/tcp

<p>Medium (CVSS: 5.9)</p> <p>NVT: SSL/TLS: Report Weak Cipher Suites</p>
<p>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.</p>
<p>Quality of Detection: 98</p>
<p>Vulnerability Detection Result ... continues on next page ...</p>

<p>...continued from previous page ...</p> <p>'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA</p> <p>'Weak' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA</p> <p>'Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA</p>
<p>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.</p>
<p>Vulnerability Insight These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808) - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000) - 1024 bit RSA authentication is considered to be insecure and therefore as weak - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong</p>
<p>Vulnerability Detection Method Details: SSL/TLS: Report Weak Cipher Suites OID:1.3.6.1.4.1.25623.1.0.103440 Version used: 2023-11-02T05:05:26Z</p>
<p>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</p>
<p>... continues on next page ...</p>

...continued from previous page ...	
cert-bund:	CB-K16/0168
cert-bund:	CB-K16/0121
cert-bund:	CB-K16/0090
cert-bund:	CB-K16/0030
cert-bund:	CB-K15/1751
cert-bund:	CB-K15/1591
cert-bund:	CB-K15/1550
cert-bund:	CB-K15/1517
cert-bund:	CB-K15/1514
cert-bund:	CB-K15/1464
cert-bund:	CB-K15/1442
cert-bund:	CB-K15/1334
cert-bund:	CB-K15/1269
cert-bund:	CB-K15/1136
cert-bund:	CB-K15/1090
cert-bund:	CB-K15/1059
cert-bund:	CB-K15/1022
cert-bund:	CB-K15/1015
cert-bund:	CB-K15/0986
cert-bund:	CB-K15/0964
cert-bund:	CB-K15/0962
cert-bund:	CB-K15/0932
cert-bund:	CB-K15/0927
cert-bund:	CB-K15/0926
cert-bund:	CB-K15/0907
cert-bund:	CB-K15/0901
cert-bund:	CB-K15/0896
cert-bund:	CB-K15/0889
cert-bund:	CB-K15/0877
cert-bund:	CB-K15/0850
cert-bund:	CB-K15/0849
cert-bund:	CB-K15/0834
cert-bund:	CB-K15/0827
cert-bund:	CB-K15/0802
cert-bund:	CB-K15/0764
cert-bund:	CB-K15/0733
cert-bund:	CB-K15/0667
cert-bund:	CB-K13/0942
dfn-cert:	DFN-CERT-2023-2939
dfn-cert:	DFN-CERT-2021-0775
dfn-cert:	DFN-CERT-2020-1561
dfn-cert:	DFN-CERT-2020-1276
dfn-cert:	DFN-CERT-2017-1821
dfn-cert:	DFN-CERT-2016-1692
dfn-cert:	DFN-CERT-2016-1648
dfn-cert:	DFN-CERT-2016-1168
dfn-cert:	DFN-CERT-2016-0665
...continues on next page ...	

...continued from previous page ...

```

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

```

Medium (CVSS: 4.3)

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

Summary

... continues on next page ...

...continued from previous page ...
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection: 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: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
Vulnerability Detection Method Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2023-10-20T16:09:12Z
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
... 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-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

... continues on next page ...

...continued from previous page ...

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
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743

...continues on next page ...

...continued from previous page ...

```
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
```

[\[return to 192.168.0.241 \]](#)**2.4.3 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: 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.

... continues on next page ...

...continued from previous page...
Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.241 \]](#)

2.5 192.168.0.252

Host scan start Sun May 5 03:01:04 2024 UTC

Host scan end Sun May 5 03:56:34 2024 UTC

Service (Port)	Threat Level
443/tcp	Medium
general/icmp	Low

2.5.1 Medium 443/tcp

Medium (CVSS: 5.9)

NVT: SSL/TLS: Report Weak Cipher Suites

Summary

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

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

Quality of Detection: 98

Vulnerability Detection Result

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

TLS_RSA_WITH_SEED_CBC_SHA

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

TLS_RSA_WITH_SEED_CBC_SHA

Solution:

Solution type: Mitigation

... continues on next page ...

...continued from previous page ...
<p>The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.</p> <p>Please see the references for more resources supporting you with this task.</p>
<p>Vulnerability Insight</p> <p>These rules are applied for the evaluation of the cryptographic strength:</p> <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
<p>Vulnerability Detection Method</p> <p>Details: SSL/TLS: Report Weak Cipher Suites</p> <p>OID:1.3.6.1.4.1.25623.1.0.103440</p> <p>Version used: 2023-11-02T05:05:26Z</p>
<p>References</p> <p>cve: CVE-2013-2566</p> <p>cve: CVE-2015-2808</p> <p>cve: CVE-2015-4000</p> <p>url: https://www.bsi.bund.de/SharedDocs/Warntmeldungen/DE/CB/warntmeldung_cb-k16-1-465_update_6.html</p> <p>url: https://bettercrypto.org/</p> <p>url: https://mozilla.github.io/server-side-tls/ssl-config-generator/</p> <p>cert-bund: CB-K21/0067</p> <p>cert-bund: CB-K19/0812</p> <p>cert-bund: CB-K17/1750</p> <p>cert-bund: CB-K16/1593</p> <p>cert-bund: CB-K16/1552</p> <p>cert-bund: CB-K16/1102</p> <p>cert-bund: CB-K16/0617</p> <p>cert-bund: CB-K16/0599</p> <p>cert-bund: CB-K16/0168</p> <p>cert-bund: CB-K16/0121</p> <p>cert-bund: CB-K16/0090</p> <p>cert-bund: CB-K16/0030</p> <p>cert-bund: CB-K15/1751</p> <p>cert-bund: CB-K15/1591</p> <p>cert-bund: CB-K15/1550</p> <p>cert-bund: CB-K15/1517</p> <p>cert-bund: CB-K15/1514</p> <p>cert-bund: CB-K15/1464</p> <p>cert-bund: CB-K15/1442</p> <p>cert-bund: CB-K15/1334</p>
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406

...continues on next page ...

...continued from previous page ...

```

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

```

Medium (CVSS: 4.3)

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

Summary

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

Quality of Detection: 98**Vulnerability Detection Result**

In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.1 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.80.2067) VT.

Impact

... continues on next page ...

...continued from previous page ...
<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>Solution:</p> <p>Solution type: 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>Affected Software/OS</p> <p>All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.</p>
<p>Vulnerability Insight</p> <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: 2023-10-20T16:09:12Z</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: 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>
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0526
 cert-bund: CB-K15/0509
 cert-bund: CB-K15/0493
 cert-bund: CB-K15/0384
 cert-bund: CB-K15/0365
 cert-bund: CB-K15/0364
 cert-bund: CB-K15/0302
 cert-bund: CB-K15/0192
 cert-bund: CB-K15/0079
 cert-bund: CB-K15/0016
 cert-bund: CB-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

...continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

[\[return to 192.168.0.252 \]](#)

2.5.2 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: 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.252 \]](#)

2.6 192.168.0.125

Host scan start Sun May 5 04:18:51 2024 UTC

Host scan end Sun May 5 05:53:12 2024 UTC

Service (Port)	Threat Level
443/tcp	Medium
135/tcp	Medium
3389/tcp	Medium
21/tcp	Medium
80/tcp	Medium
general/icmp	Low

2.6.1 Medium 443/tcp

Medium (CVSS: 5.9)

NVT: SSL/TLS: Report Weak Cipher Suites

Summary

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

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

Quality of Detection: 98

Vulnerability Detection Result

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

TLS_RSA_WITH_RC4_128_MD5

TLS_RSA_WITH_RC4_128_SHA

'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

... continues on next page ...

...continued from previous page ...
<p>These rules are applied for the evaluation of the cryptographic strength:</p> <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
<p>Vulnerability Detection Method Details: SSL/TLS: Report Weak Cipher Suites OID:1.3.6.1.4.1.25623.1.0.103440 Version used: 2023-11-02T05:05:26Z</p>
<p>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</p>
...continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0986
 cert-bund: CB-K15/0964
 cert-bund: CB-K15/0962
 cert-bund: CB-K15/0932
 cert-bund: CB-K15/0927
 cert-bund: CB-K15/0926
 cert-bund: CB-K15/0907
 cert-bund: CB-K15/0901
 cert-bund: CB-K15/0896
 cert-bund: CB-K15/0889
 cert-bund: CB-K15/0877
 cert-bund: CB-K15/0850
 cert-bund: CB-K15/0849
 cert-bund: CB-K15/0834
 cert-bund: CB-K15/0827
 cert-bund: CB-K15/0802
 cert-bund: CB-K15/0764
 cert-bund: CB-K15/0733
 cert-bund: CB-K15/0667
 cert-bund: CB-K13/0942
 dfn-cert: DFN-CERT-2023-2939
 dfn-cert: DFN-CERT-2021-0775
 dfn-cert: DFN-CERT-2020-1561
 dfn-cert: DFN-CERT-2020-1276
 dfn-cert: DFN-CERT-2017-1821
 dfn-cert: DFN-CERT-2016-1692
 dfn-cert: DFN-CERT-2016-1648
 dfn-cert: DFN-CERT-2016-1168
 dfn-cert: DFN-CERT-2016-0665
 dfn-cert: DFN-CERT-2016-0642
 dfn-cert: DFN-CERT-2016-0184
 dfn-cert: DFN-CERT-2016-0135
 dfn-cert: DFN-CERT-2016-0101
 dfn-cert: DFN-CERT-2016-0035
 dfn-cert: DFN-CERT-2015-1853
 dfn-cert: DFN-CERT-2015-1679
 dfn-cert: DFN-CERT-2015-1632
 dfn-cert: DFN-CERT-2015-1608
 dfn-cert: DFN-CERT-2015-1542
 dfn-cert: DFN-CERT-2015-1518
 dfn-cert: DFN-CERT-2015-1406
 dfn-cert: DFN-CERT-2015-1341
 dfn-cert: DFN-CERT-2015-1194
 dfn-cert: DFN-CERT-2015-1144
 dfn-cert: DFN-CERT-2015-1113
 dfn-cert: DFN-CERT-2015-1078
 dfn-cert: DFN-CERT-2015-1067

...continues on next page ...

...continued from previous page ...

```

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

```

Medium (CVSS: 5.0)

NVT: Missing 'HttpOnly' Cookie Attribute (HTTP)

Summary

The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP cookie.

Quality of Detection: 70**Vulnerability Detection Result**

The cookie(s):

Set-Cookie: ASPSESSIONIDQWRDRBCT=***replaced***; secure; path=/
is/are missing the "HttpOnly" cookie attribute.

Solution:

Solution type: Mitigation

- Set the 'HttpOnly' cookie attribute for any session cookie
- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

Affected Software/OS

Any web application with session handling in cookies.

... continues on next page ...

...continued from previous page ...
Vulnerability Insight The flaw exists if a session cookie is not using the 'HttpOnly' cookie attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.
Vulnerability Detection Method Checks all cookies sent by the remote HTTP web server / application for a missing 'HttpOnly' cookie attribute. Details: Missing 'HttpOnly' Cookie Attribute (HTTP) OID:1.3.6.1.4.1.25623.1.0.105925 Version used: 2024-01-12T16:12:12Z
References url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6 url: https://owasp.org/www-community/HttpOnly url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)
Medium (CVSS: 4.3) NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection: 98
Vulnerability Detection Result In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
Impact An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.
Solution: Solution type: Mitigation It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
... continues on next page ...

...continued from previous page ...
Affected Software/OS All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
Vulnerability Insight The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
Vulnerability Detection Method Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2023-10-20T16:09:12Z
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-K13/0845 cert-bund: CB-K13/0796
...continues on next page ...

...continued from previous page ...	
cert-bund:	CB-K13/0790
dfn-cert:	DFN-CERT-2020-0177
dfn-cert:	DFN-CERT-2020-0111
dfn-cert:	DFN-CERT-2019-0068
dfn-cert:	DFN-CERT-2018-1441
dfn-cert:	DFN-CERT-2018-1408
dfn-cert:	DFN-CERT-2016-1372
dfn-cert:	DFN-CERT-2016-1164
dfn-cert:	DFN-CERT-2016-0388
dfn-cert:	DFN-CERT-2015-1853
dfn-cert:	DFN-CERT-2015-1332
dfn-cert:	DFN-CERT-2015-0884
dfn-cert:	DFN-CERT-2015-0800
dfn-cert:	DFN-CERT-2015-0758
dfn-cert:	DFN-CERT-2015-0567
dfn-cert:	DFN-CERT-2015-0544
dfn-cert:	DFN-CERT-2015-0530
dfn-cert:	DFN-CERT-2015-0396
dfn-cert:	DFN-CERT-2015-0375
dfn-cert:	DFN-CERT-2015-0374
dfn-cert:	DFN-CERT-2015-0305
dfn-cert:	DFN-CERT-2015-0199
dfn-cert:	DFN-CERT-2015-0079
dfn-cert:	DFN-CERT-2015-0021
dfn-cert:	DFN-CERT-2014-1414
dfn-cert:	DFN-CERT-2013-1847
dfn-cert:	DFN-CERT-2013-1792
dfn-cert:	DFN-CERT-2012-1979
dfn-cert:	DFN-CERT-2012-1829
dfn-cert:	DFN-CERT-2012-1530
dfn-cert:	DFN-CERT-2012-1380
dfn-cert:	DFN-CERT-2012-1377
dfn-cert:	DFN-CERT-2012-1292
dfn-cert:	DFN-CERT-2012-1214
dfn-cert:	DFN-CERT-2012-1213
dfn-cert:	DFN-CERT-2012-1180
dfn-cert:	DFN-CERT-2012-1156
dfn-cert:	DFN-CERT-2012-1155
dfn-cert:	DFN-CERT-2012-1039
dfn-cert:	DFN-CERT-2012-0956
dfn-cert:	DFN-CERT-2012-0908
dfn-cert:	DFN-CERT-2012-0868
dfn-cert:	DFN-CERT-2012-0867
dfn-cert:	DFN-CERT-2012-0848
dfn-cert:	DFN-CERT-2012-0838
dfn-cert:	DFN-CERT-2012-0776
dfn-cert:	DFN-CERT-2012-0722
... continues on next page ...	

...continued from previous page ...

```

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

```

[\[return to 192.168.0.125 \]](#)

2.6.2 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: 80

...continues on next page ...

...continued from previous page...

Vulnerability Detection Result

Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 49664/tcp

UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
Endpoint: ncacn_ip_tcp:192.168.0.125[49664]

Port: 49665/tcp

UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
Endpoint: ncacn_ip_tcp:192.168.0.125[49665]
Annotation: DHCP Client LRPC Endpoint
UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
Endpoint: ncacn_ip_tcp:192.168.0.125[49665]
Annotation: DHCPv6 Client LRPC Endpoint
UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
Endpoint: ncacn_ip_tcp:192.168.0.125[49665]
Annotation: Event log TCPIP

Port: 49666/tcp

UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1
Endpoint: ncacn_ip_tcp:192.168.0.125[49666]
Annotation: UserMgrCli
UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
Endpoint: ncacn_ip_tcp:192.168.0.125[49666]
UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
Endpoint: ncacn_ip_tcp:192.168.0.125[49666]
Annotation: Proxy Manager provider server endpoint
UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
Endpoint: ncacn_ip_tcp:192.168.0.125[49666]
UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
Endpoint: ncacn_ip_tcp:192.168.0.125[49666]
UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
Endpoint: ncacn_ip_tcp:192.168.0.125[49666]
Annotation: IP Transition Configuration endpoint
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
Endpoint: ncacn_ip_tcp:192.168.0.125[49666]
UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
Endpoint: ncacn_ip_tcp:192.168.0.125[49666]
Annotation: IKE/Authip API
UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1
Endpoint: ncacn_ip_tcp:192.168.0.125[49666]
Annotation: UserMgrCli
UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
Endpoint: ncacn_ip_tcp:192.168.0.125[49666]
Annotation: Proxy Manager client server endpoint
UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
Endpoint: ncacn_ip_tcp:192.168.0.125[49666]
Annotation: Adh APIs
UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1

...continues on next page...

...continued from previous page...	
Endpoint: ncacn_ip_tcp:192.168.0.125[49666]	
Annotation: Impl friendly name	
Port: 49670/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_ip_tcp:192.168.0.125[49670]	
Annotation: RemoteAccessCheck	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.125[49670]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.125[49670]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.125[49670]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.125[49670]	
Annotation: KeyIso	
Port: 49684/tcp	
UUID: 0b6edbf8-4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.125[49684]	
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.125[49684]	
Named pipe : spoolss	
Win32 service or process : spoolsv.exe	
Description : Spooler service	
UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.125[49684]	
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.125[49684]	
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.125[49684]	
Port: 49703/tcp	
UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.125[49703]	
Annotation: Remote Fw APIs	
Port: 49704/tcp	
UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.125[49704]	
Port: 61807/tcp	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.125[61807]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
...continues on next page...	

...continued from previous page...
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.
Impact An attacker may use this fact to gain more knowledge about the remote host.
Solution: Solution type: Mitigation Filter incoming traffic to this ports.
Vulnerability Detection Method Details: DCE/RPC and MSRPC Services Enumeration Reporting OID:1.3.6.1.4.1.25623.1.0.10736 Version used: 2022-06-03T10:17:07Z

[\[return to 192.168.0.125 \]](#)

2.6.3 Medium 3389/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites
Summary This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.
Quality of Detection: 98
Vulnerability Detection Result 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA '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: ... continues on next page ...

...continued from previous page ...	
Solution type: Mitigation	
<p>The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.</p> <p>Please see the references for more resources supporting you with this task.</p>	
Vulnerability Insight	
<p>These rules are applied for the evaluation of the cryptographic strength:</p> <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	
<p>Details: SSL/TLS: Report Weak Cipher Suites</p> <p>OID:1.3.6.1.4.1.25623.1.0.103440</p> <p>Version used: 2023-11-02T05:05:26Z</p>	
References	
<p>cve: CVE-2013-2566</p> <p>cve: CVE-2015-2808</p> <p>cve: CVE-2015-4000</p> <p>url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1↪465_update_6.html</p> <p>url: https://bettercrypto.org/</p> <p>url: https://mozilla.github.io/server-side-tls/ssl-config-generator/</p> <p>cert-bund: CB-K21/0067</p> <p>cert-bund: CB-K19/0812</p> <p>cert-bund: CB-K17/1750</p> <p>cert-bund: CB-K16/1593</p> <p>cert-bund: CB-K16/1552</p> <p>cert-bund: CB-K16/1102</p> <p>cert-bund: CB-K16/0617</p> <p>cert-bund: CB-K16/0599</p> <p>cert-bund: CB-K16/0168</p> <p>cert-bund: CB-K16/0121</p> <p>cert-bund: CB-K16/0090</p> <p>cert-bund: CB-K16/0030</p> <p>cert-bund: CB-K15/1751</p> <p>cert-bund: CB-K15/1591</p> <p>cert-bund: CB-K15/1550</p> <p>cert-bund: CB-K15/1517</p> <p>cert-bund: CB-K15/1514</p> <p>cert-bund: CB-K15/1464</p> <p>cert-bund: CB-K15/1442</p>	
... continues on next page ...	

...continued from previous page ...

cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518

...continues on next page ...

...continued from previous page ...

```

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

```

Medium (CVSS: 4.3)

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

Summary

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

Quality of Detection: 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

... continues on next page ...

...continued from previous page ...
<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>Solution:</p> <p>Solution type: 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>Affected Software/OS</p> <p>All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.</p>
<p>Vulnerability Insight</p> <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: 2023-10-20T16:09:12Z</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: 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>
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-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

...continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

[\[return to 192.168.0.125 \]](#)

2.6.4 Medium 21/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login
Summary The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
Quality of Detection: 70
Vulnerability Detection Result The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↩. Response(s): Non-anonymous sessions: 331 Password required Anonymous sessions: 331 Password required
Impact An attacker can uncover login names and passwords by sniffing traffic to the FTP service.
Solution: Solution type: Mitigation Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.
Vulnerability Detection Method Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command. Details: FTP Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.108528 Version used: 2023-12-20T05:05:58Z

[\[return to 192.168.0.125 \]](#)

2.6.5 Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Missing 'HttpOnly' Cookie Attribute (HTTP)
Summary The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP cookie.
...
... continues on next page ...

...continued from previous page ...
Quality of Detection: 70
Vulnerability Detection Result The cookie(s): Set-Cookie: ASPSESSIONIDQSRDRBCT=***replaced***; path=/ is/are missing the "HttpOnly" cookie attribute.
Solution: Solution type: Mitigation - Set the 'HttpOnly' cookie attribute for any session cookie - Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)
Affected Software/OS Any web application with session handling in cookies.
Vulnerability Insight The flaw exists if a session cookie is not using the 'HttpOnly' cookie attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.
Vulnerability Detection Method Checks all cookies sent by the remote HTTP web server / application for a missing 'HttpOnly' cookie attribute. Details: Missing 'HttpOnly' Cookie Attribute (HTTP) OID:1.3.6.1.4.1.25623.1.0.105925 Version used: 2024-01-12T16:12:12Z
References url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6 url: https://owasp.org/www-community/HttpOnly url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0↪02)

[\[return to 192.168.0.125 \]](#)

2.6.6 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
Summary The remote host responded to an ICMP timestamp request.
... continues on next page ...

...continued from previous page ...
Quality of Detection: 80
Vulnerability Detection Result The following response / ICMP packet has been received: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.125 \]](#)

2.7 192.168.0.143

Host scan start Sun May 5 04:46:55 2024 UTC
Host scan end Sun May 5 05:30:44 2024 UTC

Service (Port)	Threat Level
135/tcp	Medium
3389/tcp	Medium
general/icmp	Low

2.7.1 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: 80

Vulnerability Detection Result

Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 49432/tcp

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

Endpoint: ncacn_ip_tcp:192.168.0.143[49432]

Named pipe : lsass

Win32 service or process : lsass.exe

Description : SAM access

Port: 49664/tcp

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

Endpoint: ncacn_ip_tcp:192.168.0.143[49664]

Port: 49665/tcp

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

Endpoint: ncacn_ip_tcp:192.168.0.143[49665]

Annotation: Event log TCPIP

Port: 49667/tcp

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

Endpoint: ncacn_ip_tcp:192.168.0.143[49667]

Annotation: RemoteAccessCheck

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

Endpoint: ncacn_ip_tcp:192.168.0.143[49667]

Named pipe : lsass

Win32 service or process : lsass.exe

Description : SAM access

UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1

Endpoint: ncacn_ip_tcp:192.168.0.143[49667]

Annotation: Ngc Pop Key Service

... continues on next page ...

...continued from previous page...	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.143[49667]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.143[49667]	
Annotation: KeyIso	
Port: 49669/tcp	
UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.143[49669]	
Annotation: UserMgrCli	
UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.143[49669]	
UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.143[49669]	
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.143[49669]	
UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.143[49669]	
Annotation: IKE/Authip API	
UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.143[49669]	
Annotation: UserMgrCli	
UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.143[49669]	
Annotation: Adh APIs	
Port: 49670/tcp	
UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.143[49670]	
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.143[49670]	
Named pipe : spoolss	
Win32 service or process : spoolsv.exe	
Description : Spooler service	
UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.143[49670]	
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.143[49670]	
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.143[49670]	
Port: 49711/tcp	
UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.143[49711]	
Annotation: Remote Fw APIs	
Port: 49713/tcp	
UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.143[49713]	
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re	
...continues on next page...	

...continued from previous page ...
↳porting this list is not enabled by default due to the possible large size of ↳this list. See the script preferences to enable this reporting.
Impact An attacker may use this fact to gain more knowledge about the remote host.
Solution: Solution type: Mitigation Filter incoming traffic to this ports.
Vulnerability Detection Method Details: DCE/RPC and MSRPC Services Enumeration Reporting OID:1.3.6.1.4.1.25623.1.0.10736 Version used: 2022-06-03T10:17:07Z

[\[return to 192.168.0.143 \]](#)

2.7.2 Medium 3389/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites
Summary This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.
Quality of Detection: 98
Vulnerability Detection Result 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA '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
... continues on next page ...

...continued from previous page ...
<p>The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.</p> <p>Please see the references for more resources supporting you with this task.</p>
<p>Vulnerability Insight</p> <p>These rules are applied for the evaluation of the cryptographic strength:</p> <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
<p>Vulnerability Detection Method</p> <p>Details: SSL/TLS: Report Weak Cipher Suites</p> <p>OID:1.3.6.1.4.1.25623.1.0.103440</p> <p>Version used: 2023-11-02T05:05:26Z</p>
<p>References</p> <p>cve: CVE-2013-2566</p> <p>cve: CVE-2015-2808</p> <p>cve: CVE-2015-4000</p> <p>url: https://www.bsi.bund.de/SharedDocs/Warntmeldungen/DE/CB/warntmeldung_cb-k16-1-465_update_6.html</p> <p>url: https://bettercrypto.org/</p> <p>url: https://mozilla.github.io/server-side-tls/ssl-config-generator/</p> <p>cert-bund: CB-K21/0067</p> <p>cert-bund: CB-K19/0812</p> <p>cert-bund: CB-K17/1750</p> <p>cert-bund: CB-K16/1593</p> <p>cert-bund: CB-K16/1552</p> <p>cert-bund: CB-K16/1102</p> <p>cert-bund: CB-K16/0617</p> <p>cert-bund: CB-K16/0599</p> <p>cert-bund: CB-K16/0168</p> <p>cert-bund: CB-K16/0121</p> <p>cert-bund: CB-K16/0090</p> <p>cert-bund: CB-K16/0030</p> <p>cert-bund: CB-K15/1751</p> <p>cert-bund: CB-K15/1591</p> <p>cert-bund: CB-K15/1550</p> <p>cert-bund: CB-K15/1517</p> <p>cert-bund: CB-K15/1514</p> <p>cert-bund: CB-K15/1464</p> <p>cert-bund: CB-K15/1442</p> <p>cert-bund: CB-K15/1334</p>
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406

...continues on next page ...

...continued from previous page ...

```

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

```

Medium (CVSS: 4.3)

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

Summary

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

Quality of Detection: 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

... continues on next page ...

...continued from previous page ...
<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>Solution:</p> <p>Solution type: 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>Affected Software/OS</p> <p>All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.</p>
<p>Vulnerability Insight</p> <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: 2023-10-20T16:09:12Z</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: 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>
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-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

...continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

[\[return to 192.168.0.143 \]](#)

2.7.3 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: 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.143 \]](#)

2.8 192.168.0.202

Host scan start Sun May 5 03:02:51 2024 UTC

Host scan end Sun May 5 04:10:01 2024 UTC

Service (Port)	Threat Level
3389/tcp	Medium
135/tcp	Medium
general/icmp	Low

2.8.1 Medium 3389/tcp

Medium (CVSS: 5.9)

NVT: SSL/TLS: Report Weak Cipher Suites

Summary

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

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

Quality of Detection: 98

Vulnerability Detection Result

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

TLS_RSA_WITH_RC4_128_MD5

TLS_RSA_WITH_RC4_128_SHA

'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)

... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - 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: 2023-11-02T05:05:26Z
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
...continues on next page ...

...continued from previous page ...

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-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016

...continues on next page ...

...continued from previous page ...

```

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

```

Medium (CVSS: 4.3)

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

Summary

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

Quality of Detection: 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 ...
Affected Software/OS All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
Vulnerability Insight The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
Vulnerability Detection Method Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2023-10-20T16:09:12Z
References cve: CVE-2011-3389 cve: CVE-2015-0204 url: https://ssl-config.mozilla.org/ url: https://bettercrypto.org/ url: https://datatracker.ietf.org/doc/rfc8996/ url: https://vnhacker.blogspot.com/2011/09/beast.html url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters ↔-report-2014 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K18/0799 cert-bund: CB-K16/1289 cert-bund: CB-K16/1096 cert-bund: CB-K15/1751 cert-bund: CB-K15/1266 cert-bund: CB-K15/0850 cert-bund: CB-K15/0764 cert-bund: CB-K15/0720 cert-bund: CB-K15/0548 cert-bund: CB-K15/0526 cert-bund: CB-K15/0509 cert-bund: CB-K15/0493 cert-bund: CB-K15/0384 cert-bund: CB-K15/0365 cert-bund: CB-K15/0364 cert-bund: CB-K15/0302 cert-bund: CB-K15/0192 cert-bund: CB-K15/0079 cert-bund: CB-K15/0016
...continues on next page ...

...continued from previous page ...

cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838

... continues on next page ...

...continued from previous page ...	
dfn-cert:	DFN-CERT-2012-0776
dfn-cert:	DFN-CERT-2012-0722
dfn-cert:	DFN-CERT-2012-0638
dfn-cert:	DFN-CERT-2012-0627
dfn-cert:	DFN-CERT-2012-0451
dfn-cert:	DFN-CERT-2012-0418
dfn-cert:	DFN-CERT-2012-0354
dfn-cert:	DFN-CERT-2012-0234
dfn-cert:	DFN-CERT-2012-0221
dfn-cert:	DFN-CERT-2012-0177
dfn-cert:	DFN-CERT-2012-0170
dfn-cert:	DFN-CERT-2012-0146
dfn-cert:	DFN-CERT-2012-0142
dfn-cert:	DFN-CERT-2012-0126
dfn-cert:	DFN-CERT-2012-0123
dfn-cert:	DFN-CERT-2012-0095
dfn-cert:	DFN-CERT-2012-0051
dfn-cert:	DFN-CERT-2012-0047
dfn-cert:	DFN-CERT-2012-0021
dfn-cert:	DFN-CERT-2011-1953
dfn-cert:	DFN-CERT-2011-1946
dfn-cert:	DFN-CERT-2011-1844
dfn-cert:	DFN-CERT-2011-1826
dfn-cert:	DFN-CERT-2011-1774
dfn-cert:	DFN-CERT-2011-1743
dfn-cert:	DFN-CERT-2011-1738
dfn-cert:	DFN-CERT-2011-1706
dfn-cert:	DFN-CERT-2011-1628
dfn-cert:	DFN-CERT-2011-1627
dfn-cert:	DFN-CERT-2011-1619
dfn-cert:	DFN-CERT-2011-1482

[\[return to 192.168.0.202 \]](#)

2.8.2 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.
... continues on next page ...

...continued from previous page...

Quality of Detection: 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: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
Endpoint: ncacn_ip_tcp:192.168.0.202[49664]

Port: 49665/tcp

UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
Endpoint: ncacn_ip_tcp:192.168.0.202[49665]
Annotation: DHCP Client LRPC Endpoint
UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
Endpoint: ncacn_ip_tcp:192.168.0.202[49665]
Annotation: DHCPv6 Client LRPC Endpoint
UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
Endpoint: ncacn_ip_tcp:192.168.0.202[49665]
Annotation: Event log TCPIP

Port: 49666/tcp

UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1
Endpoint: ncacn_ip_tcp:192.168.0.202[49666]
Annotation: UserMgrCli
UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
Endpoint: ncacn_ip_tcp:192.168.0.202[49666]
UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
Endpoint: ncacn_ip_tcp:192.168.0.202[49666]
Annotation: Proxy Manager provider server endpoint
UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
Endpoint: ncacn_ip_tcp:192.168.0.202[49666]
UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
Endpoint: ncacn_ip_tcp:192.168.0.202[49666]
Annotation: IP Transition Configuration endpoint
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
Endpoint: ncacn_ip_tcp:192.168.0.202[49666]
UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
Endpoint: ncacn_ip_tcp:192.168.0.202[49666]
Annotation: IKE/Authip API
UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1
Endpoint: ncacn_ip_tcp:192.168.0.202[49666]
Annotation: UserMgrCli
UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
Endpoint: ncacn_ip_tcp:192.168.0.202[49666]
Annotation: Proxy Manager client server endpoint
UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
Endpoint: ncacn_ip_tcp:192.168.0.202[49666]
Annotation: Adh APIs
UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1

...continues on next page...

...continued from previous page...	
Endpoint: ncacn_ip_tcp:192.168.0.202[49666]	
Annotation: Impl friendly name	
Port: 49669/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_ip_tcp:192.168.0.202[49669]	
Annotation: RemoteAccessCheck	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.202[49669]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.202[49669]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.202[49669]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.202[49669]	
Annotation: KeyIso	
Port: 49676/tcp	
UUID: 0b6edbf-a4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.202[49676]	
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.202[49676]	
Named pipe : spoolss	
Win32 service or process : spoolsv.exe	
Description : Spooler service	
UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.202[49676]	
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.202[49676]	
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.202[49676]	
Port: 49703/tcp	
UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.202[49703]	
Annotation: Remote Fw APIs	
Port: 49706/tcp	
UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.202[49706]	
Port: 49725/tcp	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.202[49725]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
...continues on next page...	

...continued from previous page...
<p>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.</p>
<p>Impact An attacker may use this fact to gain more knowledge about the remote host.</p>
<p>Solution: Solution type: Mitigation Filter incoming traffic to this ports.</p>
<p>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</p>

[\[return to 192.168.0.202 \]](#)

2.8.3 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<p>Summary The remote host responded to an ICMP timestamp request.</p>
Quality of Detection: 80
<p>Vulnerability Detection Result The following response / ICMP packet has been received:</p> <ul style="list-style-type: none"> - ICMP Type: 14 - ICMP Code: 0
<p>Impact This information could theoretically be used to exploit weak time-based random number generators in other services.</p>
<p>Solution: Solution type: Mitigation Various mitigations are possible:</p> <ul style="list-style-type: none"> - 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[[return to 192.168.0.202](#)]

2.9 192.168.0.168

Host scan start Sun May 5 03:46:04 2024 UTC
Host scan end Sun May 5 05:05:01 2024 UTC

Service (Port)	Threat Level
3389/tcp	Medium
135/tcp	Medium
general/icmp	Low

2.9.1 Medium 3389/tcp

Medium (CVSS: 5.9) NVT: SSL/TLS: Report Weak Cipher Suites
Summary This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.
... continues on next page ...

...continued from previous page ...
Quality of Detection: 98
Vulnerability Detection Result 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA '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) - 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: 2023-11-02T05:05:26Z
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
... continues on next page ...

...continued from previous page ...	
cert-bund:	CB-K16/1552
cert-bund:	CB-K16/1102
cert-bund:	CB-K16/0617
cert-bund:	CB-K16/0599
cert-bund:	CB-K16/0168
cert-bund:	CB-K16/0121
cert-bund:	CB-K16/0090
cert-bund:	CB-K16/0030
cert-bund:	CB-K15/1751
cert-bund:	CB-K15/1591
cert-bund:	CB-K15/1550
cert-bund:	CB-K15/1517
cert-bund:	CB-K15/1514
cert-bund:	CB-K15/1464
cert-bund:	CB-K15/1442
cert-bund:	CB-K15/1334
cert-bund:	CB-K15/1269
cert-bund:	CB-K15/1136
cert-bund:	CB-K15/1090
cert-bund:	CB-K15/1059
cert-bund:	CB-K15/1022
cert-bund:	CB-K15/1015
cert-bund:	CB-K15/0986
cert-bund:	CB-K15/0964
cert-bund:	CB-K15/0962
cert-bund:	CB-K15/0932
cert-bund:	CB-K15/0927
cert-bund:	CB-K15/0926
cert-bund:	CB-K15/0907
cert-bund:	CB-K15/0901
cert-bund:	CB-K15/0896
cert-bund:	CB-K15/0889
cert-bund:	CB-K15/0877
cert-bund:	CB-K15/0850
cert-bund:	CB-K15/0849
cert-bund:	CB-K15/0834
cert-bund:	CB-K15/0827
cert-bund:	CB-K15/0802
cert-bund:	CB-K15/0764
cert-bund:	CB-K15/0733
cert-bund:	CB-K15/0667
cert-bund:	CB-K13/0942
dfn-cert:	DFN-CERT-2023-2939
dfn-cert:	DFN-CERT-2021-0775
dfn-cert:	DFN-CERT-2020-1561
dfn-cert:	DFN-CERT-2020-1276
dfn-cert:	DFN-CERT-2017-1821
...continues on next page ...	

...continued from previous page...

dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection: 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: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
Vulnerability Detection Method Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2023-10-20T16:09:12Z
References cve: CVE-2011-3389 cve: CVE-2015-0204 ... continues on next page ...

...continued from previous page ...

```

url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↔-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-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

```

... continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953

...continues on next page ...

...continued from previous page ...

```
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
```

[\[return to 192.168.0.168 \]](#)**2.9.2 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: 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: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1

Endpoint: ncacn_ip_tcp:192.168.0.168[49664]

Port: 49665/tcp

UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1

Endpoint: ncacn_ip_tcp:192.168.0.168[49665]

Annotation: NRP server endpoint

UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1

Endpoint: ncacn_ip_tcp:192.168.0.168[49665]

Annotation: DHCP Client LRPC Endpoint

UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1

Endpoint: ncacn_ip_tcp:192.168.0.168[49665]

Annotation: DHCPv6 Client LRPC Endpoint

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

Endpoint: ncacn_ip_tcp:192.168.0.168[49665]

... continues on next page ...

...continued from previous page...
<p>Annotation: Event log TCPIP</p> <p>Port: 49666/tcp</p> <p>UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.168[49666]</p> <p>Annotation: RemoteAccessCheck</p> <p>UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.168[49666]</p> <p>Named pipe : lsass</p> <p>Win32 service or process : lsass.exe</p> <p>Description : SAM access</p> <p>UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.168[49666]</p> <p>Annotation: Ngc Pop Key Service</p> <p>UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.168[49666]</p> <p>Annotation: Ngc Pop Key Service</p> <p>UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.168[49666]</p> <p>Annotation: KeyIso</p> <p>Port: 49667/tcp</p> <p>UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.168[49667]</p> <p>Annotation: UserMgrCli</p> <p>UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.168[49667]</p> <p>Annotation: AppInfo</p> <p>UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.168[49667]</p> <p>UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.168[49667]</p> <p>Annotation: Proxy Manager provider server endpoint</p> <p>UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.168[49667]</p> <p>UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.168[49667]</p> <p>Annotation: IP Transition Configuration endpoint</p> <p>UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.168[49667]</p> <p>Annotation: AppInfo</p> <p>UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.168[49667]</p> <p>Annotation: AppInfo</p> <p>UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.168[49667]</p> <p>UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1</p> <p>Endpoint: ncacn_ip_tcp:192.168.0.168[49667]</p> <p>Annotation: IKE/Authip API</p>
...continues on next page...

...continued from previous page...	
UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.168[49667]	
Annotation: UserMgrCli	
UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.168[49667]	
Annotation: Proxy Manager client server endpoint	
UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.168[49667]	
Annotation: Adh APIs	
UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.168[49667]	
Annotation: Impl friendly name	
UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.168[49667]	
Annotation: AppInfo	
UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.168[49667]	
Annotation: AppInfo	
Port: 49686/tcp	
UUID: 0b6edbf8-4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.168[49686]	
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.168[49686]	
Named pipe : spoolss	
Win32 service or process : spoolsv.exe	
Description : Spooler service	
UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.168[49686]	
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.168[49686]	
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.168[49686]	
Port: 49707/tcp	
UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.168[49707]	
Annotation: Remote Fw APIs	
Port: 49710/tcp	
UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.168[49710]	
Port: 61855/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_ip_tcp:192.168.0.168[61855]	
Annotation: RemoteAccessCheck	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.168[61855]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
...continues on next page...	

<p>...continued from previous page ...</p> <p>Description : SAM access UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1 Endpoint: ncacn_ip_tcp:192.168.0.168[61855] Annotation: Ngc Pop Key Service UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:192.168.0.168[61855] Annotation: Ngc Pop Key Service UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:192.168.0.168[61855] Annotation: KeyIso</p> <p>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.</p>
<p>Impact An attacker may use this fact to gain more knowledge about the remote host.</p>
<p>Solution: Solution type: Mitigation Filter incoming traffic to this ports.</p>
<p>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</p>

[\[return to 192.168.0.168 \]](#)

2.9.3 Low general/icmp

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

...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: 2023-05-11T09:09:33Z

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

dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.168 \]](#)

2.10 192.168.0.250

Host scan start Sun May 5 03:01:04 2024 UTC

Host scan end Sun May 5 04:45:54 2024 UTC

Service (Port)	Threat Level
135/tcp	Medium
3389/tcp	Medium
general/icmp	Low

2.10.1 Medium 135/tcp

Medium (CVSS: 5.0)

NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary

Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Quality of Detection: 80

Vulnerability Detection Result

Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 11731/tcp

UUID: d107c6e0-fc35-49ba-ba03-3e192de6797d, version 1

Endpoint: ncacn_ip_tcp:192.168.0.250[11731]

Annotation: Veeam Deployer

UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1

Endpoint: ncacn_ip_tcp:192.168.0.250[11731]

Annotation: Veeam RPC Invoker

Port: 49664/tcp

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

Endpoint: ncacn_ip_tcp:192.168.0.250[49664]

Port: 49665/tcp

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

Endpoint: ncacn_ip_tcp:192.168.0.250[49665]

Annotation: Event log TCPIP

Port: 49669/tcp

UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1

Endpoint: ncacn_ip_tcp:192.168.0.250[49669]

Annotation: UserMgrCli

UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1

Endpoint: ncacn_ip_tcp:192.168.0.250[49669]

Annotation: AppInfo

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

Endpoint: ncacn_ip_tcp:192.168.0.250[49669]

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

Endpoint: ncacn_ip_tcp:192.168.0.250[49669]

Annotation: Proxy Manager provider server endpoint

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

Endpoint: ncacn_ip_tcp:192.168.0.250[49669]

UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1

Endpoint: ncacn_ip_tcp:192.168.0.250[49669]

Annotation: AppInfo

UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1

Endpoint: ncacn_ip_tcp:192.168.0.250[49669]

Annotation: AppInfo

... continues on next page ...

...continued from previous page...	
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49669]	
UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49669]	
Annotation: IKE/Authip API	
UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49669]	
Annotation: UserMgrCli	
UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49669]	
Annotation: Proxy Manager client server endpoint	
UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49669]	
Annotation: Adh APIs	
UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49669]	
UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49669]	
Annotation: AppInfo	
UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49669]	
Annotation: AppInfo	
Port: 49670/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_ip_tcp:192.168.0.250[49670]	
Annotation: RemoteAccessCheck	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49670]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49670]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49670]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.250[49670]	
Annotation: KeyIso	
Port: 49672/tcp	
UUID: 0b6edbf8-4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49672]	
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49672]	
Named pipe : spoolss	
Win32 service or process : spoolsv.exe	
...continues on next page...	

...continued from previous page...	
Description : Spooler service	
UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49672]	
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49672]	
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49672]	
Port: 49718/tcp	
UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[49718]	
Annotation: Remote Fw APIs	
Port: 49722/tcp	
UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.250[49722]	
Port: 52838/tcp	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[52838]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
Port: 6160/tcp	
UUID: d107c6e0-fc35-49ba-ba03-3e192de6797d, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[6160]	
Annotation: Veeam Deployer	
UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[6160]	
Annotation: Veeam RPC Invoker	
Port: 6161/tcp	
UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[6161]	
Annotation: Veeam Invoker	
Port: 6162/tcp	
UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[6162]	
Annotation: Veeam Invoker	
Port: 6190/tcp	
UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[6190]	
Annotation: Veeam Invoker	
Port: 6210/tcp	
UUID: 844d6366-6a97-4eb5-8345-b88e8276c20d, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[6210]	
Annotation: Veeam HV Integration	
UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.250[6210]	
Annotation: Veeam Invoker	
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re	
...continues on next page...	

...continued from previous page...
↳porting this list is not enabled by default due to the possible large size of ↳this list. See the script preferences to enable this reporting.
Impact An attacker may use this fact to gain more knowledge about the remote host.
Solution: Solution type: Mitigation Filter incoming traffic to this ports.
Vulnerability Detection Method Details: DCE/RPC and MSRPC Services Enumeration Reporting OID:1.3.6.1.4.1.25623.1.0.10736 Version used: 2022-06-03T10:17:07Z

[\[return to 192.168.0.250 \]](#)

2.10.2 Medium 3389/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites
Summary This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.
Quality of Detection: 98
Vulnerability Detection Result 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA '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
... continues on next page ...

...continued from previous page ...
<p>The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.</p> <p>Please see the references for more resources supporting you with this task.</p>
<p>Vulnerability Insight</p> <p>These rules are applied for the evaluation of the cryptographic strength:</p> <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
<p>Vulnerability Detection Method</p> <p>Details: SSL/TLS: Report Weak Cipher Suites</p> <p>OID:1.3.6.1.4.1.25623.1.0.103440</p> <p>Version used: 2023-11-02T05:05:26Z</p>
<p>References</p> <p>cve: CVE-2013-2566</p> <p>cve: CVE-2015-2808</p> <p>cve: CVE-2015-4000</p> <p>url: https://www.bsi.bund.de/SharedDocs/Warntmeldungen/DE/CB/warntmeldung_cb-k16-1-465_update_6.html</p> <p>url: https://bettercrypto.org/</p> <p>url: https://mozilla.github.io/server-side-tls/ssl-config-generator/</p> <p>cert-bund: CB-K21/0067</p> <p>cert-bund: CB-K19/0812</p> <p>cert-bund: CB-K17/1750</p> <p>cert-bund: CB-K16/1593</p> <p>cert-bund: CB-K16/1552</p> <p>cert-bund: CB-K16/1102</p> <p>cert-bund: CB-K16/0617</p> <p>cert-bund: CB-K16/0599</p> <p>cert-bund: CB-K16/0168</p> <p>cert-bund: CB-K16/0121</p> <p>cert-bund: CB-K16/0090</p> <p>cert-bund: CB-K16/0030</p> <p>cert-bund: CB-K15/1751</p> <p>cert-bund: CB-K15/1591</p> <p>cert-bund: CB-K15/1550</p> <p>cert-bund: CB-K15/1517</p> <p>cert-bund: CB-K15/1514</p> <p>cert-bund: CB-K15/1464</p> <p>cert-bund: CB-K15/1442</p> <p>cert-bund: CB-K15/1334</p>
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406

...continues on next page ...

...continued from previous page ...

```

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

```

Medium (CVSS: 4.3)

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

Summary

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

Quality of Detection: 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

... continues on next page ...

...continued from previous page ...
<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>Solution:</p> <p>Solution type: 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>Affected Software/OS</p> <p>All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.</p>
<p>Vulnerability Insight</p> <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: 2023-10-20T16:09:12Z</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: 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>
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0526
 cert-bund: CB-K15/0509
 cert-bund: CB-K15/0493
 cert-bund: CB-K15/0384
 cert-bund: CB-K15/0365
 cert-bund: CB-K15/0364
 cert-bund: CB-K15/0302
 cert-bund: CB-K15/0192
 cert-bund: CB-K15/0079
 cert-bund: CB-K15/0016
 cert-bund: CB-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

...continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

[\[return to 192.168.0.250 \]](#)

2.10.3 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: 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.250 \]](#)

2.11 192.168.0.65

Host scan start Sun May 5 03:02:18 2024 UTC

Host scan end Sun May 5 03:48:37 2024 UTC

Service (Port)	Threat Level
21/tcp	Medium
3389/tcp	Medium
135/tcp	Medium
general/icmp	Low

2.11.1 Medium 21/tcp

Medium (CVSS: 4.8)

NVT: FTP Unencrypted Cleartext Login

Summary

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

Quality of Detection: 70

Vulnerability Detection Result

The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↩. Response(s):

Non-anonymous sessions: 331 Please, specify the password.

Anonymous sessions: 331 Please, specify the password.

Impact

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

Solution:

Solution type: Mitigation

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

Vulnerability Detection Method

Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.

Details: FTP Unencrypted Cleartext Login

OID:1.3.6.1.4.1.25623.1.0.108528

Version used: 2023-12-20T05:05:58Z

[\[return to 192.168.0.65 \]](#)

2.11.2 Medium 3389/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites
<p>Summary</p> <p>This routine reports all Weak SSL/TLS cipher suites accepted by a service.</p> <p>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.</p>
Quality of Detection: 98
<p>Vulnerability Detection Result</p> <p>'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:</p> <p>TLS_RSA_WITH_RC4_128_MD5</p> <p>TLS_RSA_WITH_RC4_128_SHA</p> <p>'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:</p> <p>TLS_RSA_WITH_RC4_128_MD5</p> <p>TLS_RSA_WITH_RC4_128_SHA</p> <p>'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:</p> <p>TLS_RSA_WITH_RC4_128_MD5</p> <p>TLS_RSA_WITH_RC4_128_SHA</p>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.</p> <p>Please see the references for more resources supporting you with this task.</p>
<p>Vulnerability Insight</p> <p>These rules are applied for the evaluation of the cryptographic strength:</p> <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
<p>Vulnerability Detection Method</p> <p>Details: SSL/TLS: Report Weak Cipher Suites</p> <p>OID:1.3.6.1.4.1.25623.1.0.103440</p> <p>Version used: 2023-11-02T05:05:26Z</p>
References
... continues on next page ...

...continued from previous page ...

```
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
    ↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
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
```

... continues on next page ...

...continued from previous page ...

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-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879

...continues on next page ...

...continued from previous page ...
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.
Quality of Detection: 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: - 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: 2023-10-20T16:09:12Z</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: 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-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</p>
...continues on next page ...

...continued from previous page ...

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

...continues on next page ...

...continued from previous page ...

```

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

```

[\[return to 192.168.0.65 \]](#)

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

Endpoint: ncacn_ip_tcp:192.168.0.65[49664]

Port: 49665/tcp

UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1

Endpoint: ncacn_ip_tcp:192.168.0.65[49665]

Annotation: DHCP Client LRPC Endpoint

...continues on next page ...

...continued from previous page...	
UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49665]	
Annotation: DHCPv6 Client LRPC Endpoint	
UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49665]	
Annotation: Event log TCPIP	
Port: 49668/tcp	
UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
Annotation: UserMgrCli	
UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
Annotation: AppInfo	
UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
Annotation: Proxy Manager provider server endpoint	
UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
Annotation: IP Transition Configuration endpoint	
UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
Annotation: AppInfo	
UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
Annotation: AppInfo	
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
Annotation: IKE/Authip API	
UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
Annotation: UserMgrCli	
UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
Annotation: Proxy Manager client server endpoint	
UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
Annotation: Adh APIs	
UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
...continues on next page...	

...continued from previous page...	
Annotation: Impl friendly name	
UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
Annotation: AppInfo	
UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49668]	
Annotation: AppInfo	
Port: 49675/tcp	
UUID: 0b6edbf8-4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49675]	
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49675]	
Named pipe : spoolss	
Win32 service or process : spoolsv.exe	
Description : Spooler service	
UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49675]	
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49675]	
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49675]	
Port: 49683/tcp	
UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49683]	
Annotation: Remote Fw APIs	
Port: 49712/tcp	
UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.65[49712]	
Port: 49746/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_ip_tcp:192.168.0.65[49746]	
Annotation: RemoteAccessCheck	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49746]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49746]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[49746]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.65[49746]	
...continues on next page...	

...continued from previous page...	
Annotation: KeyIso	
Port: 56666/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_ip_tcp:192.168.0.65[56666]	
Annotation: RemoteAccessCheck	
Port: 6160/tcp	
UUID: d107c6e0-fc35-49ba-ba03-3e192de6797d, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[6160]	
Annotation: Veeam Deployer	
UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[6160]	
Annotation: Veeam RPC Invoker	
Port: 6162/tcp	
UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[6162]	
Annotation: Veeam Invoker	
Port: 6190/tcp	
UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.65[6190]	
Annotation: Veeam Invoker	
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.	
Impact	
An attacker may use this fact to gain more knowledge about the remote host.	
Solution:	
Solution type: Mitigation	
Filter incoming traffic to this ports.	
Vulnerability Detection Method	
Details: DCE/RPC and MSRPC Services Enumeration Reporting	
OID:1.3.6.1.4.1.25623.1.0.10736	
Version used: 2022-06-03T10:17:07Z	

[\[return to 192.168.0.65 \]](#)

2.11.4 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
...
... continues on next page ...

...continued from previous page...
Summary The remote host responded to an ICMP timestamp request.
Quality of Detection: 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.65 \]](#)

2.12 192.168.0.3

Host scan start Sun May 5 03:01:04 2024 UTC
Host scan end Sun May 5 03:42:08 2024 UTC

Service (Port)	Threat Level
3389/tcp	Medium
135/tcp	Medium
general/icmp	Low

2.12.1 Medium 3389/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites
<p>Summary</p> <p>This routine reports all Weak SSL/TLS cipher suites accepted by a service.</p> <p>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.</p>
<p>Quality of Detection: 98</p>
<p>Vulnerability Detection Result</p> <p>'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:</p> <p>TLS_RSA_WITH_RC4_128_MD5</p> <p>TLS_RSA_WITH_RC4_128_SHA</p> <p>'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:</p> <p>TLS_RSA_WITH_RC4_128_MD5</p> <p>TLS_RSA_WITH_RC4_128_SHA</p> <p>'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:</p> <p>TLS_RSA_WITH_RC4_128_MD5</p> <p>TLS_RSA_WITH_RC4_128_SHA</p>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.</p> <p>Please see the references for more resources supporting you with this task.</p>
<p>Vulnerability Insight</p> <p>These rules are applied for the evaluation of the cryptographic strength:</p> <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
... continues on next page ...

...continued from previous page ...

Vulnerability Detection Method

Details: SSL/TLS: Report Weak Cipher Suites

OID:1.3.6.1.4.1.25623.1.0.103440

Version used: 2023-11-02T05:05:26Z

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.htmlurl: <https://bettercrypto.org/>url: <https://mozilla.github.io/server-side-tls/ssl-config-generator/>

cert-bund: CB-K21/0067

cert-bund: CB-K19/0812

cert-bund: CB-K17/1750

cert-bund: CB-K16/1593

cert-bund: CB-K16/1552

cert-bund: CB-K16/1102

cert-bund: CB-K16/0617

cert-bund: CB-K16/0599

cert-bund: CB-K16/0168

cert-bund: CB-K16/0121

cert-bund: CB-K16/0090

cert-bund: CB-K16/0030

cert-bund: CB-K15/1751

cert-bund: CB-K15/1591

cert-bund: CB-K15/1550

cert-bund: CB-K15/1517

cert-bund: CB-K15/1514

cert-bund: CB-K15/1464

cert-bund: CB-K15/1442

cert-bund: CB-K15/1334

cert-bund: CB-K15/1269

cert-bund: CB-K15/1136

cert-bund: CB-K15/1090

cert-bund: CB-K15/1059

cert-bund: CB-K15/1022

cert-bund: CB-K15/1015

cert-bund: CB-K15/0986

cert-bund: CB-K15/0964

cert-bund: CB-K15/0962

cert-bund: CB-K15/0932

cert-bund: CB-K15/0927

cert-bund: CB-K15/0926

cert-bund: CB-K15/0907

cert-bund: CB-K15/0901

... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956

...continues on next page ...

...continued from previous page ...

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

Medium (CVSS: 4.3)

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

Summary

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

Quality of Detection: 98**Vulnerability Detection Result**

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

Impact

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

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

Solution:**Solution type:** Mitigation

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

Affected Software/OS

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

Vulnerability Insight

... continues on next page ...

...continued from previous page ...
<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: 2023-10-20T16:09:12Z</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: 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-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> <p>dfn-cert: DFN-CERT-2019-0068</p>
...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418

...continues on next page ...

...continued from previous page ...

```

dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482

```

[\[return to 192.168.0.3 \]](#)**2.12.2 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: 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

...continues on next page ...

...continued from previous page...	
UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49664]	
Port: 49665/tcp	
UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49665]	
Annotation: NRP server endpoint	
UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49665]	
Annotation: DHCP Client LRPC Endpoint	
UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49665]	
Annotation: DHCPv6 Client LRPC Endpoint	
UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49665]	
Annotation: Event log TCPIP	
Port: 49666/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_ip_tcp:192.168.0.3[49666]	
Annotation: RemoteAccessCheck	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49666]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49666]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49666]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.3[49666]	
Annotation: KeyIso	
Port: 49667/tcp	
UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49667]	
Annotation: UserMgrCli	
UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49667]	
Annotation: AppInfo	
UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49667]	
UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49667]	
Annotation: Proxy Manager provider server endpoint	
UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49667]	
...continues on next page...	

...continued from previous page...	
UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49667]	
Annotation: IP Transition Configuration endpoint	
UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49667]	
Annotation: AppInfo	
UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49667]	
Annotation: AppInfo	
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49667]	
UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49667]	
Annotation: IKE/Authip API	
UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49667]	
Annotation: UserMgrCli	
UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49667]	
Annotation: Proxy Manager client server endpoint	
UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49667]	
Annotation: Adh APIs	
UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49667]	
Annotation: Impl friendly name	
UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49667]	
Annotation: AppInfo	
UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49667]	
Annotation: AppInfo	
Port: 49668/tcp	
UUID: 0b6edbf8-4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49668]	
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49668]	
Named pipe : spoolss	
Win32 service or process : spoolsv.exe	
Description : Spooler service	
UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49668]	
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49668]	
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.3[49668]	
Port: 49669/tcp	
...continues on next page...	

...continued from previous page...	
UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1 Endpoint: ncacn_ip_tcp:192.168.0.3[49669] Annotation: Remote Fw APIs Port: 49674/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:192.168.0.3[49674] Port: 57213/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:192.168.0.3[57213] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1 Endpoint: ncacn_ip_tcp:192.168.0.3[57213] Annotation: Ngc Pop Key Service UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:192.168.0.3[57213] Annotation: Ngc Pop Key Service UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:192.168.0.3[57213] Annotation: KeyIso 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.	
Impact	An attacker may use this fact to gain more knowledge about the remote host.
Solution:	
Solution type: Mitigation	Filter incoming traffic to this ports.
Vulnerability Detection Method	
Details: DCE/RPC and MSRPC Services Enumeration Reporting	
OID:1.3.6.1.4.1.25623.1.0.10736	
Version used: 2022-06-03T10:17:07Z	

[\[return to 192.168.0.3 \]](#)

2.12.3 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: 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.3 \]](#)

2.13 192.168.0.220

Host scan start Sun May 5 04:59:19 2024 UTC
 Host scan end Sun May 5 05:38:46 2024 UTC

Service (Port)	Threat Level
135/tcp	Medium
3389/tcp	Medium
general/icmp	Low

2.13.1 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: 80

Vulnerability Detection Result

Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 11731/tcp

UUID: d107c6e0-fc35-49ba-ba03-3e192de6797d, version 1

Endpoint: ncacn_ip_tcp:192.168.0.220[11731]

Annotation: Veeam Deployer

UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1

Endpoint: ncacn_ip_tcp:192.168.0.220[11731]

Annotation: Veeam RPC Invoker

Port: 49664/tcp

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

Endpoint: ncacn_ip_tcp:192.168.0.220[49664]

Port: 49665/tcp

UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1

Endpoint: ncacn_ip_tcp:192.168.0.220[49665]

Annotation: DHCP Client LRPC Endpoint

UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1

Endpoint: ncacn_ip_tcp:192.168.0.220[49665]

Annotation: DHCPv6 Client LRPC Endpoint

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

Endpoint: ncacn_ip_tcp:192.168.0.220[49665]

Annotation: Event log TCPIP

... continues on next page ...

...continued from previous page...

Port: 49666/tcp
 UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
 Endpoint: ncacn_ip_tcp:192.168.0.220[49666]
 Annotation: RemoteAccessCheck
 UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
 Endpoint: ncacn_ip_tcp:192.168.0.220[49666]
 Named pipe : lsass
 Win32 service or process : lsass.exe
 Description : SAM access
 UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
 Endpoint: ncacn_ip_tcp:192.168.0.220[49666]
 Annotation: Ngc Pop Key Service
 UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
 Endpoint: ncacn_ip_tcp:192.168.0.220[49666]
 Annotation: Ngc Pop Key Service
 UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
 Endpoint: ncacn_ip_tcp:192.168.0.220[49666]
 Annotation: KeyIso

Port: 49667/tcp
 UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1
 Endpoint: ncacn_ip_tcp:192.168.0.220[49667]
 Annotation: UserMgrCli
 UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1
 Endpoint: ncacn_ip_tcp:192.168.0.220[49667]
 Annotation: AppInfo
 UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
 Endpoint: ncacn_ip_tcp:192.168.0.220[49667]
 UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
 Endpoint: ncacn_ip_tcp:192.168.0.220[49667]
 Annotation: Proxy Manager provider server endpoint
 UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
 Endpoint: ncacn_ip_tcp:192.168.0.220[49667]
 UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
 Endpoint: ncacn_ip_tcp:192.168.0.220[49667]
 Annotation: IP Transition Configuration endpoint
 UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1
 Endpoint: ncacn_ip_tcp:192.168.0.220[49667]
 Annotation: AppInfo
 UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1
 Endpoint: ncacn_ip_tcp:192.168.0.220[49667]
 Annotation: AppInfo
 UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
 Endpoint: ncacn_ip_tcp:192.168.0.220[49667]
 UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
 Endpoint: ncacn_ip_tcp:192.168.0.220[49667]
 Annotation: IKE/Authip API
 UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1

...continues on next page...

...continued from previous page...	
Endpoint: ncacn_ip_tcp:192.168.0.220[49667]	
Annotation: UserMgrCli	
UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.220[49667]	
Annotation: Proxy Manager client server endpoint	
UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.220[49667]	
Annotation: Adh APIs	
UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.220[49667]	
Annotation: Impl friendly name	
UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.220[49667]	
UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.220[49667]	
Annotation: AppInfo	
UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.220[49667]	
Annotation: AppInfo	
Port: 49668/tcp	
UUID: 0b6edbf4-4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.220[49668]	
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.220[49668]	
Named pipe : spoolss	
Win32 service or process : spoolsv.exe	
Description : Spooler service	
UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.220[49668]	
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.220[49668]	
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.220[49668]	
Port: 49669/tcp	
UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.220[49669]	
Port: 49688/tcp	
UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.220[49688]	
Annotation: Remote Fw APIs	
Port: 6160/tcp	
UUID: d107c6e0-fc35-49ba-ba03-3e192de6797d, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.220[6160]	
Annotation: Veeam Deployer	
UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.220[6160]	
Annotation: Veeam RPC Invoker	
...continues on next page...	

...continued from previous page...	
Port: 6162/tcp	UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1 Endpoint: ncacn_ip_tcp:192.168.0.220[6162] Annotation: Veeam Invoker
Port: 6190/tcp	UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1 Endpoint: ncacn_ip_tcp:192.168.0.220[6190] Annotation: Veeam Invoker
Port: 6210/tcp	UUID: 844d6366-6a97-4eb5-8345-b88e8276c20d, version 1 Endpoint: ncacn_ip_tcp:192.168.0.220[6210] Annotation: Veeam HV Integration UUID: d1c2c07a-d989-48cc-a423-b73ecd518d40, version 1 Endpoint: ncacn_ip_tcp:192.168.0.220[6210] Annotation: Veeam Invoker
Port: 62638/tcp	UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:192.168.0.220[62638] Annotation: RemoteAccessCheck UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:192.168.0.220[62638] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access
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.	
Impact An attacker may use this fact to gain more knowledge about the remote host.	
Solution: Solution type: Mitigation Filter incoming traffic to this ports.	
Vulnerability Detection Method Details: DCE/RPC and MSRPC Services Enumeration Reporting OID:1.3.6.1.4.1.25623.1.0.10736 Version used: 2022-06-03T10:17:07Z	

[\[return to 192.168.0.220 \]](#)

2.13.2 Medium 3389/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites
<p>Summary</p> <p>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.</p>
Quality of Detection: 98
<p>Vulnerability Detection Result</p> <p>'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA</p> <p>'Weak' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA</p> <p>'Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA</p>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>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.</p>
<p>Vulnerability Insight</p> <p>These rules are applied for the evaluation of the cryptographic strength:</p> <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
<p>Vulnerability Detection Method</p> <p>Details: SSL/TLS: Report Weak Cipher Suites OID:1.3.6.1.4.1.25623.1.0.103440 Version used: 2023-11-02T05:05:26Z</p>
<p>References</p> <p>cve: CVE-2013-2566 cve: CVE-2015-2808</p>
... continues on next page ...

...continued from previous page ...

cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1↔465_update_6.html
url: <https://bettercrypto.org/>
url: <https://mozilla.github.io/server-side-tls/ssl-config-generator/>
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
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

... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0764
 cert-bund: CB-K15/0733
 cert-bund: CB-K15/0667
 cert-bund: CB-K13/0942
 dfn-cert: DFN-CERT-2023-2939
 dfn-cert: DFN-CERT-2021-0775
 dfn-cert: DFN-CERT-2020-1561
 dfn-cert: DFN-CERT-2020-1276
 dfn-cert: DFN-CERT-2017-1821
 dfn-cert: DFN-CERT-2016-1692
 dfn-cert: DFN-CERT-2016-1648
 dfn-cert: DFN-CERT-2016-1168
 dfn-cert: DFN-CERT-2016-0665
 dfn-cert: DFN-CERT-2016-0642
 dfn-cert: DFN-CERT-2016-0184
 dfn-cert: DFN-CERT-2016-0135
 dfn-cert: DFN-CERT-2016-0101
 dfn-cert: DFN-CERT-2016-0035
 dfn-cert: DFN-CERT-2015-1853
 dfn-cert: DFN-CERT-2015-1679
 dfn-cert: DFN-CERT-2015-1632
 dfn-cert: DFN-CERT-2015-1608
 dfn-cert: DFN-CERT-2015-1542
 dfn-cert: DFN-CERT-2015-1518
 dfn-cert: DFN-CERT-2015-1406
 dfn-cert: DFN-CERT-2015-1341
 dfn-cert: DFN-CERT-2015-1194
 dfn-cert: DFN-CERT-2015-1144
 dfn-cert: DFN-CERT-2015-1113
 dfn-cert: DFN-CERT-2015-1078
 dfn-cert: DFN-CERT-2015-1067
 dfn-cert: DFN-CERT-2015-1038
 dfn-cert: DFN-CERT-2015-1016
 dfn-cert: DFN-CERT-2015-1012
 dfn-cert: DFN-CERT-2015-0980
 dfn-cert: DFN-CERT-2015-0977
 dfn-cert: DFN-CERT-2015-0976
 dfn-cert: DFN-CERT-2015-0960
 dfn-cert: DFN-CERT-2015-0956
 dfn-cert: DFN-CERT-2015-0944
 dfn-cert: DFN-CERT-2015-0937
 dfn-cert: DFN-CERT-2015-0925
 dfn-cert: DFN-CERT-2015-0884
 dfn-cert: DFN-CERT-2015-0881
 dfn-cert: DFN-CERT-2015-0879
 dfn-cert: DFN-CERT-2015-0866
 dfn-cert: DFN-CERT-2015-0844

...continues on next page ...

...continued from previous page ...

```
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.

Quality of Detection: 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:

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

Vulnerability Detection Method

Check the used TLS protocols of the services provided by this system.

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

... continues on next page ...

...continued from previous page ...	
OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2023-10-20T16:09:12Z	
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-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	
...continues on next page ...	

...continued from previous page ...

dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126

...continues on next page ...

...continued from previous page ...

```

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

```

[\[return to 192.168.0.220 \]](#)

2.13.3 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: 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)
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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[[return to 192.168.0.220](#)]

2.14 192.168.0.254

Host scan start Sun May 5 03:01:25 2024 UTC
Host scan end Sun May 5 04:25:22 2024 UTC

Service (Port)	Threat Level
443/tcp	Medium

2.14.1 Medium 443/tcp

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits
Summary The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.
Quality of Detection: 80
... continues on next page ...

...continued from previous page ...	
Vulnerability Detection Result The remote SSL/TLS server is using the following certificate(s) with a RSA key with less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer): 1024:RSA:6634E4C5:CN=www.brocade.com,OU=Brocade Communications Systems,O=Brocade Communications Systems,L=Santa Clara,ST=California,C=US (Server certificate)	
Impact Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.	
Solution: Solution type: Mitigation Replace the certificate with a stronger key and reissue the certificates it signed.	
Vulnerability Insight SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.	
Vulnerability Detection Method Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit. Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048. ↳.. OID:1.3.6.1.4.1.25623.1.0.150710 Version used: 2021-12-10T12:48:00Z	
References url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf	

Medium (CVSS: 5.0)	
NVT: SSL/TLS: 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: 70	
Vulnerability Detection Result The following indicates that the remote SSL/TLS service is affected: Protocol Version Successful re-done SSL/TLS handshakes (Renegotiation) over an ↳ existing / already established SSL/TLS connection ----- ↳----- TLSv1.0 10	
... continues on next page ...	

...continued from previous page ...	
TLSv1.1	10
TLSv1.2	10
Impact The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.	
Solution: Solution type: VendorFix Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.	
Affected Software/OS Every SSL/TLS service which does not properly restrict client-initiated renegotiation.	
Vulnerability Insight The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols. Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale: > It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment. Both CVEs are still kept in this VT as a reference to the origin of this flaw.	
Vulnerability Detection Method Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection. Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) OID:1.3.6.1.4.1.25623.1.0.117761 Version used: 2024-02-02T05:06:11Z	
References cve: CVE-2011-1473 cve: CVE-2011-5094 url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/ url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/ url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation url: https://www.openwall.com/lists/oss-security/2011/07/08/2 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K17/0980 cert-bund: CB-K17/0979 cert-bund: CB-K13/0915 cert-bund: CB-K13/0462 dfn-cert: DFN-CERT-2017-1013	
... continues on next page ...	

...continued from previous page ...

```
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112
```

Medium (CVSS: 4.3)

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

Summary

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

Quality of Detection: 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:

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

Vulnerability Detection Method

Check the used TLS protocols of the services provided by this system.

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

... continues on next page ...

...continued from previous page ...	
OID:1.3.6.1.4.1.25623.1.0.117274	
Version used: 2023-10-20T16:09:12Z	
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-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	
...continues on next page ...	

...continued from previous page ...

dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126

...continues on next page ...

...continued from previous page ...

```

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

```

Medium (CVSS: 4.0)

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

Summary

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

Quality of Detection: 80**Vulnerability Detection Result**

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

Subject: CN=www.brocade.com,OU=Brocade Communications Systems,O=Brocade Communications Systems,L=Santa Clara,ST=California,C=US

Signature Algorithm: sha1WithRSAEncryption

Solution:**Solution type:** Mitigation

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

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)

... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - Message Digest 5 (MD5) - Message Digest 4 (MD4) - Message Digest 2 (MD2) <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>Vulnerability Detection Method</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> <p>Version used: 2021-10-15T11:13:32Z</p>
<p>References</p> <p>url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/</p>

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
<p>Summary</p> <p>The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).</p>
Quality of Detection: 80
<p>Vulnerability Detection Result</p> <p>Server Temporary Key Size: 1024 bits</p>
<p>Impact</p> <p>An attacker might be able to decrypt the SSL/TLS communication offline.</p>
<p>Solution:</p> <p>Solution type: Workaround</p> <p>Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).</p> <p>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.</p>
... continues on next page ...

...continued from previous page ...

Vulnerability Insight

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

Vulnerability Detection Method

Checks the DHE temporary public key size.

Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability.
↔...

OID:1.3.6.1.4.1.25623.1.0.106223

Version used: 2023-07-21T05:05:22Z

References

url: <https://weakdh.org/>

url: <https://weakdh.org/sysadmin.html>

[\[return to 192.168.0.254 \]](#)

2.15 192.168.0.15

Host scan start Sun May 5 04:58:09 2024 UTC

Host scan end Sun May 5 15:19:03 2024 UTC

Service (Port)	Threat Level
25/tcp	Medium
22/tcp	Medium
443/tcp	Medium
22/tcp	Low
general/icmp	Low

2.15.1 Medium 25/tcp

Medium (CVSS: 5.0)

NVT: Check if Mailserver answer to VRFY and EXPN requests

Summary

The Mailserver on this host answers to VRFY and/or EXPN requests.

Quality of Detection: 99

Vulnerability Detection Result

'VRFY root' produces the following answer: 252 2.0.0 root

... continues on next page ...

...continued from previous page ...
Solution: Solution type: Workaround Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.
Vulnerability Insight VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.
Vulnerability Detection Method Details: Check if Mailserver answer to VRFY and EXPN requests OID:1.3.6.1.4.1.25623.1.0.100072 Version used: 2023-10-31T05:06:37Z
References url: http://cr.yp.to/smtp/vrfy.html

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: 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 ----- ↔----- TLSh1.0 10 TLSh1.1 10 TLSh1.2 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: ... continues on next page ...

...continued from previous page...	
Solution type: VendorFix	Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.
Affected Software/OS	Every SSL/TLS service which does not properly restrict client-initiated renegotiation.
Vulnerability Insight	<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>> 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>
Vulnerability Detection Method	<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: 2024-02-02T05:06:11Z</p>
References	<p>cve: CVE-2011-1473</p> <p>cve: CVE-2011-5094</p> <p>url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</p> <p>url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</p> <p>url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</p> <p>url: https://www.openwall.com/lists/oss-security/2011/07/08/2</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-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>

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: 70
Vulnerability Detection Result The following indicates that the remote SSL/TLS service is affected: Protocol Version Successful re-done SSL/TLS handshakes (Renegotiation) over an ↪ existing / already established SSL/TLS connection ----- ↪----- TLSv1.0 10 TLSv1.1 10 TLSv1.2 10
Impact The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.
Solution: Solution type: VendorFix Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.
Affected Software/OS Every SSL/TLS service which does not properly restrict client-initiated renegotiation.
Vulnerability Insight The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols. Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale: > It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment. Both CVEs are still kept in this VT as a reference to the origin of this flaw.
Vulnerability Detection Method Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection. Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) OID:1.3.6.1.4.1.25623.1.0.117761
... continues on next page ...

...continued from previous page ...
Version used: 2024-02-02T05:06:11Z
References cve: CVE-2011-1473 cve: CVE-2011-5094 url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego-mitigation-dos/ url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/ url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation url: https://www.openwall.com/lists/oss-security/2011/07/08/2 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K17/0980 cert-bund: CB-K17/0979 cert-bund: CB-K13/0915 cert-bund: CB-K13/0462 dfn-cert: DFN-CERT-2017-1013 dfn-cert: DFN-CERT-2017-1012 dfn-cert: DFN-CERT-2014-0809 dfn-cert: DFN-CERT-2013-1928 dfn-cert: DFN-CERT-2012-1112

Medium (CVSS: 5.0)
NVT: Check if Mailserver answer to VRFY and EXPN requests
Summary The Mailserver on this host answers to VRFY and/or EXPN requests.
Quality of Detection: 99
Vulnerability Detection Result 'VRFY root' produces the following answer: 252 2.0.0 root
Solution: Solution type: Workaround Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.
Vulnerability Insight VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Details: Check if Mailserver answer to VRFY and EXPN requests OID:1.3.6.1.4.1.25623.1.0.100072 Version used: 2023-10-31T05:06:37Z
References url: http://cr.yp.to/smtp/vrfy.html

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection: 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: - 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)
... continues on next page ...

...continued from previous page ...

Vulnerability Detection Method

Check the used TLS protocols of the services provided by this system.

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

OID:1.3.6.1.4.1.25623.1.0.117274

Version used: 2023-10-20T16:09:12Z

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-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

...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

```

[\[return to 192.168.0.15 \]](#)**2.15.2 Medium 22/tcp**

Medium (CVSS: 5.3)

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

Summary

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

Quality of Detection: 80**Vulnerability Detection Result**

The remote SSH server supports the following weak KEX algorithm(s):

KEX algorithm | Reason

```

-----
gss-gex-sha1-      | Using SHA-1
gss-group14-sha1-  | Deprecated algorithm, e.g. using SHA-1

```

Impact

An attacker can quickly break individual connections.

Solution:

... continues on next page ...

...continued from previous page ...

Solution type: Mitigation

Disable the reported weak KEX algorithm(s)

- 1024-bit MODP group / prime KEX algorithms:

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

Vulnerability Insight

- 1024-bit MODP group / prime KEX algorithms:

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

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

Vulnerability Detection Method

Checks the supported KEX algorithms of the remote SSH server.

Currently weak KEX algorithms are defined as the following:

- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime

- ephemerally generated key exchange groups uses SHA-1

- using RSA 1024-bit modulus key

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

OID:1.3.6.1.4.1.25623.1.0.150713

Version used: 2023-10-12T05:05:32Z

References

url: <https://weakdh.org/sysadmin.html>

url: <https://www.rfc-editor.org/rfc/rfc9142>

url: <https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem>

url: <https://www.rfc-editor.org/rfc/rfc6194>

url: <https://www.rfc-editor.org/rfc/rfc4253#section-6.5>

[\[return to 192.168.0.15 \]](#)

2.15.3 Medium 443/tcp

Medium (CVSS: 5.0)

NVT: Missing 'Secure' Cookie Attribute (HTTP)

Summary

The remote HTTP web server / application is missing to set the 'Secure' cookie attribute for one or more sent HTTP cookie.

Quality of Detection: 70

... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result The cookie(s): Set-Cookie: PHPSESSID=***replaced***; path=/ is/are missing the "Secure" cookie attribute.
Solution: Solution type: Mitigation - Set the 'Secure' cookie attribute for any cookies that are sent over a SSL/TLS connection - Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)
Affected Software/OS Any web application accessible via a SSL/TLS connection (HTTPS) and at the same time also accessible over a cleartext connection (HTTP).
Vulnerability Insight The flaw exists if a cookie is not using the 'Secure' cookie attribute and is sent over a SSL/TLS connection. This allows a cookie to be passed to the server by the client over non-secure channels (HTTP) and subsequently allows an attacker to e.g. conduct session hijacking attacks.
Vulnerability Detection Method Checks all cookies sent by the remote HTTP web server / application over a SSL/TLS connection for a missing 'Secure' cookie attribute. Details: Missing 'Secure' Cookie Attribute (HTTP) OID:1.3.6.1.4.1.25623.1.0.902661 Version used: 2024-01-12T16:12:12Z
References url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.5 url: https://owasp.org/www-community/controls/SecureCookieAttribute url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0↪02)
Medium (CVSS: 5.0) NVT: Missing 'HttpOnly' Cookie Attribute (HTTP)
Summary The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP cookie.
Quality of Detection: 70
Vulnerability Detection Result ... continues on next page ...

...continued from previous page ...
<p>The cookie(s): Set-Cookie: PHPSESSID=***replaced***; path=/ is/are missing the "HttpOnly" cookie attribute.</p>
<p>Solution: Solution type: Mitigation</p> <ul style="list-style-type: none">- Set the 'HttpOnly' cookie attribute for any session cookie- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)
<p>Affected Software/OS Any web application with session handling in cookies.</p>
<p>Vulnerability Insight The flaw exists if a session cookie is not using the 'HttpOnly' cookie attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.</p>
<p>Vulnerability Detection Method Checks all cookies sent by the remote HTTP web server / application for a missing 'HttpOnly' cookie attribute. Details: Missing 'HttpOnly' Cookie Attribute (HTTP) OID:1.3.6.1.4.1.25623.1.0.105925 Version used: 2024-01-12T16:12:12Z</p>
<p>References url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6 url: https://owasp.org/www-community/HttpOnly url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0↪02)</p>

[\[return to 192.168.0.15 \]](#)

2.15.4 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)
<p>Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).</p>
<p>Quality of Detection: 80</p>
<p>Vulnerability Detection Result ... continues on next page ...</p>

<p>...continued from previous page ...</p> <p>The remote SSH server supports the following weak client-to-server MAC algorithm $\hookrightarrow(s)$:</p> <p>umac-64-etm@openssh.com umac-64@openssh.com</p> <p>The remote SSH server supports the following weak server-to-client MAC algorithm $\hookleftarrow(s)$:</p> <p>umac-64-etm@openssh.com umac-64@openssh.com</p>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>Disable the reported weak MAC algorithm(s).</p>
<p>Vulnerability Detection Method</p> <p>Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.</p> <p>Currently weak MAC algorithms are defined as the following:</p> <ul style="list-style-type: none"> - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm <p>Details: Weak MAC Algorithm(s) Supported (SSH)</p> <p>OID:1.3.6.1.4.1.25623.1.0.105610</p> <p>Version used: 2023-10-12T05:05:32Z</p>
<p>References</p> <p>url: https://www.rfc-editor.org/rfc/rfc6668</p> <p>url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4</p>

[\[return to 192.168.0.15 \]](#)

2.15.5 Low general/icmp

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

...continued from previous page ...	
- 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.15 \]](#)

2.16 192.168.0.249

Host scan start Sun May 5 03:48:29 2024 UTC
Host scan end Sun May 5 05:00:12 2024 UTC

Service (Port)	Threat Level
22/tcp	Medium
general/icmp	Low

2.16.1 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)
Summary The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).
Quality of Detection: 80
Vulnerability Detection Result The remote SSH server supports the following weak KEX algorithm(s): KEX algorithm Reason ----- diffie-hellman-group-exchange-sha1 Using SHA-1
Impact An attacker can quickly break individual connections.
Solution: Solution type: Mitigation Disable the reported weak KEX algorithm(s) - 1024-bit MODP group / prime KEX algorithms: Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.
Vulnerability Insight - 1024-bit MODP group / prime KEX algorithms: Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime. A nation-state can break a 1024-bit prime.
Vulnerability Detection Method Checks the supported KEX algorithms of the remote SSH server. Currently weak KEX algorithms are defined as the following: - non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime - ephemerally generated key exchange groups uses SHA-1 - using RSA 1024-bit modulus key Details: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.150713 Version used: 2023-10-12T05:05:32Z
References url: https://weakdh.org/sysadmin.html url: https://www.rfc-editor.org/rfc/rfc9142 url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implementations ... continues on next page ...

...continued from previous page ...

url: <https://www.rfc-editor.org/rfc/rfc6194>url: <https://www.rfc-editor.org/rfc/rfc4253#section-6.5>

Medium (CVSS: 4.3)

NVT: Weak Encryption Algorithm(s) Supported (SSH)

Summary

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

Quality of Detection: 80**Vulnerability Detection Result**

The remote SSH server supports the following weak client-to-server encryption algorithm(s):

aes128-cbc

aes256-cbc

The remote SSH server supports the following weak server-to-client encryption algorithm(s):

aes128-cbc

aes256-cbc

Solution:**Solution type:** Mitigation

Disable the reported weak encryption algorithm(s).

Vulnerability Insight

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

Vulnerability Detection Method

Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.

Currently weak encryption algorithms are defined as the following:

- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms

Details: Weak Encryption Algorithm(s) Supported (SSH)

OID:1.3.6.1.4.1.25623.1.0.105611

... continues on next page ...

...continued from previous page ...
Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc8758 url: https://www.kb.cert.org/vuls/id/958563 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3

[\[return to 192.168.0.249 \]](#)

2.16.2 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: 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.
... continues on next page ...

...continued from previous page ...
Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[[return to 192.168.0.249](#)]

2.17 192.168.0.201

Host scan start Sun May 5 04:28:34 2024 UTC
Host scan end Sun May 5 05:15:59 2024 UTC

Service (Port)	Threat Level
22/tcp	Medium
80/tcp	Medium
22/tcp	Low
general/icmp	Low

2.17.1 Medium 22/tcp

Medium (CVSS: 5.3) NVT: Weak Host Key Algorithm(s) (SSH)
Summary The remote SSH server is configured to allow / support weak host key algorithm(s).
Quality of Detection: 80
Vulnerability Detection Result The remote SSH server supports the following weak host key algorithm(s): host key algorithm Description ----- ↪----- ssh-dss Digital Signature Algorithm (DSA) / Digital Signature Stand ↪ard (DSS)
Solution:
... continues on next page ...

...continued from previous page ...
Solution type: Mitigation Disable the reported weak host key algorithm(s).
Vulnerability Detection Method Checks the supported host key algorithms of the remote SSH server. Currently weak host key algorithms are defined as the following: - ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS) Details: Weak Host Key Algorithm(s) (SSH) OID:1.3.6.1.4.1.25623.1.0.117687 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc8332 url: https://www.rfc-editor.org/rfc/rfc8709 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6

[\[return to 192.168.0.201 \]](#)

2.17.2 Medium 80/tcp

Medium (CVSS: 4.8) NVT: Cleartext Transmission of Sensitive Information via HTTP
Summary The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.
Quality of Detection: 80
Vulnerability Detection Result The following input fields were identified (URL:input name): http://192.168.0.201/:password
Impact An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.
Solution: Solution type: Workaround Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.
... continues on next page ...

...continued from previous page ...

Affected Software/OS

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

Vulnerability Detection Method

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.

The script is currently checking the following:

- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'

Details: Cleartext Transmission of Sensitive Information via HTTP

OID:1.3.6.1.4.1.25623.1.0.108440

Version used: 2023-09-07T05:05:21Z

References

url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management

url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure

url: <https://cwe.mitre.org/data/definitions/319.html>

[\[return to 192.168.0.201 \]](#)

2.17.3 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

The remote SSH server supports the following weak client-to-server MAC algorithm(s):

umac-64-etm@openssh.com

umac-64@openssh.com

The remote SSH server supports the following weak server-to-client MAC algorithm(s):

umac-64-etm@openssh.com

umac-64@openssh.com

... continues on next page ...

...continued from previous page ...
Solution: Solution type: Mitigation Disable the reported weak MAC algorithm(s).
Vulnerability Detection Method Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: <ul style="list-style-type: none"> - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[[return to 192.168.0.201](#)]

2.17.4 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: 80
Vulnerability Detection Result The following response / ICMP packet has been received: <ul style="list-style-type: none"> - 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
... continues on next page ...

...continued from previous page ...

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: 2023-05-11T09:09:33Z

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

dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.201 \]](#)

2.18 192.168.0.2

Host scan start Sun May 5 03:01:04 2024 UTC

Host scan end Sun May 5 04:46:55 2024 UTC

Service (Port)	Threat Level
443/tcp	Medium
general/icmp	Low
22/tcp	Low

2.18.1 Medium 443/tcp

Medium (CVSS: 5.0)

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

Summary

... continues on next page ...

...continued from previous page ...
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.
Quality of Detection: 70
Vulnerability Detection Result The following indicates that the remote SSL/TLS service is affected: Protocol Version Successful re-done SSL/TLS handshakes (Renegotiation) over an ↔ existing / already established SSL/TLS connection ----- ↔----- TLSv1.2 10
Impact The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.
Solution: Solution type: VendorFix Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.
Affected Software/OS Every SSL/TLS service which does not properly restrict client-initiated renegotiation.
Vulnerability Insight The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols. Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale: > It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment. Both CVEs are still kept in this VT as a reference to the origin of this flaw.
Vulnerability Detection Method Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection. Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) OID:1.3.6.1.4.1.25623.1.0.117761 Version used: 2024-02-02T05:06:11Z
References cve: CVE-2011-1473 cve: CVE-2011-5094 url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/
... continues on next page ...

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

Medium (CVSS: 5.0)
NVT: SSL/TLS: 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: 70
Vulnerability Detection Result The following indicates that the remote SSL/TLS service is affected: Protocol Version Successful re-done SSL/TLS handshakes (Renegotiation) over an ↪ existing / already established SSL/TLS connection ----- ↪----- TLSv1.2 10
Impact The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.
Solution: Solution type: VendorFix Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.
Affected Software/OS Every SSL/TLS service which does not properly restrict client-initiated renegotiation.
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
<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>> 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>
<p>Vulnerability Detection Method</p> <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: 2024-02-02T05:06:11Z</p>
<p>References</p> <p>cve: CVE-2011-1473</p> <p>cve: CVE-2011-5094</p> <p>url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</p> <p>url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</p> <p>url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</p> <p>url: https://www.openwall.com/lists/oss-security/2011/07/08/2</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-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>

[\[return to 192.168.0.2 \]](#)

2.18.2 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<p>Summary</p> <p>The remote host responded to an ICMP timestamp request.</p>
... continues on next page ...

...continued from previous page...	
Quality of Detection: 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: 2023-05-11T09:09:33Z	
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 dfn-cert: DFN-CERT-2014-0658	

[\[return to 192.168.0.2 \]](#)

2.18.3 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)
Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).
Quality of Detection: 80
Vulnerability Detection Result The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s): umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm ↪(s): umac-64-etm@openssh.com umac-64@openssh.com
Solution: Solution type: Mitigation Disable the reported weak MAC algorithm(s).
Vulnerability Detection Method Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[\[return to 192.168.0.2 \]](#)

2.19 192.168.0.16

Host scan start Sun May 5 05:00:13 2024 UTC
Host scan end Sun May 5 05:58:25 2024 UTC

Service (Port)	Threat Level
135/tcp	Medium
general/icmp	Low

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

Endpoint: ncacn_ip_tcp:192.168.0.16[49664]

Port: 49665/tcp

UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1

Endpoint: ncacn_ip_tcp:192.168.0.16[49665]

Annotation: DHCP Client LRPC Endpoint

UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1

Endpoint: ncacn_ip_tcp:192.168.0.16[49665]

Annotation: DHCPv6 Client LRPC Endpoint

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

Endpoint: ncacn_ip_tcp:192.168.0.16[49665]

Annotation: Event log TCPIP

Port: 49668/tcp

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

Endpoint: ncacn_ip_tcp:192.168.0.16[49668]

Annotation: RemoteAccessCheck

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

Endpoint: ncacn_ip_tcp:192.168.0.16[49668]

Named pipe : lsass

Win32 service or process : Netlogon

Description : Net Logon service

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

Endpoint: ncacn_ip_tcp:192.168.0.16[49668]

Named pipe : lsass

Win32 service or process : lsass.exe

... continues on next page ...

...continued from previous page...	
Description : LSA access	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49668]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49668]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49668]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.16[49668]	
Annotation: KeyIso	
UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49668]	
Annotation: Impl friendly name	
UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4	
Endpoint: ncacn_ip_tcp:192.168.0.16[49668]	
Annotation: MS NT Directory DRS Interface	
UUID: f5cc5a18-4264-101a-8c59-08002b2f8426, version 56	
Endpoint: ncacn_ip_tcp:192.168.0.16[49668]	
Annotation: MS NT Directory NSP Interface	
Port: 49671/tcp	
UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
Annotation: UserMgrCli	
UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
Annotation: AppInfo	
UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
Annotation: Proxy Manager provider server endpoint	
UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
Annotation: IP Transition Configuration endpoint	
UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
Annotation: AppInfo	
UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1	
...continues on next page...	

...continued from previous page...	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
Annotation: AppInfo	
UUID: 7d814569-35b3-4850-bb32-83035fceb6e, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
Annotation: IAS RPC server	
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
Annotation: IKE/Authip API	
UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
Annotation: UserMgrCli	
UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
Annotation: Proxy Manager client server endpoint	
UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
Annotation: Adh APIs	
UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
Annotation: Impl friendly name	
UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
Annotation: AppInfo	
UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49671]	
Annotation: AppInfo	
Port: 49678/tcp	
UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49678]	
Annotation: Remote Fw APIs	
Port: 49695/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_http:192.168.0.16[49695]	
Annotation: RemoteAccessCheck	
UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1	
Endpoint: ncacn_http:192.168.0.16[49695]	
Named pipe : lsass	
Win32 service or process : Netlogon	
Description : Net Logon service	
UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0	
Endpoint: ncacn_http:192.168.0.16[49695]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
...continues on next page...	

...continued from previous page...	
Description : LSA access	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_http:192.168.0.16[49695]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_http:192.168.0.16[49695]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_http:192.168.0.16[49695]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_http:192.168.0.16[49695]	
Annotation: KeyIso	
UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4	
Endpoint: ncacn_http:192.168.0.16[49695]	
Annotation: MS NT Directory DRS Interface	
UUID: f5cc5a18-4264-101a-8c59-08002b2f8426, version 56	
Endpoint: ncacn_http:192.168.0.16[49695]	
Annotation: MS NT Directory NSP Interface	
Port: 49696/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_ip_tcp:192.168.0.16[49696]	
Annotation: RemoteAccessCheck	
UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49696]	
Named pipe : lsass	
Win32 service or process : Netlogon	
Description : Net Logon service	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49696]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49696]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49696]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.16[49696]	
Annotation: KeyIso	
Port: 49701/tcp	
UUID: 0b6edbf-a4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.16[49701]	
...continues on next page...	

...continued from previous page...	
<p> UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:192.168.0.16[49701] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:192.168.0.16[49701] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:192.168.0.16[49701] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:192.168.0.16[49701] </p> <p>Port: 50391/tcp</p> <p> UUID: a00c021c-2be2-11d2-b678-0000f87a8f8e, version 1 Endpoint: ncacn_ip_tcp:192.168.0.16[50391] Annotation: PERFMON SERVICE UUID: d049b186-814f-11d1-9a3c-00c04fc9b232, version 1 Endpoint: ncacn_ip_tcp:192.168.0.16[50391] Annotation: NtFrs API UUID: f5cc59b4-4264-101a-8c59-08002b2f8426, version 1 Endpoint: ncacn_ip_tcp:192.168.0.16[50391] Annotation: NtFrs Service </p> <p>Port: 50404/tcp</p> <p> UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:192.168.0.16[50404] </p> <p>Port: 50525/tcp</p> <p> UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5 Endpoint: ncacn_ip_tcp:192.168.0.16[50525] Named pipe : dnsserver Win32 service or process : dns.exe Description : DNS Server </p> <p>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.</p>	
Impact	An attacker may use this fact to gain more knowledge about the remote host.
Solution:	
Solution type: Mitigation	Filter incoming traffic to this ports.
Vulnerability Detection Method	
Details: DCE/RPC and MSRPC Services Enumeration Reporting	
OID:1.3.6.1.4.1.25623.1.0.10736	
Version used: 2022-06-03T10:17:07Z	

[\[return to 192.168.0.16 \]](#)

2.19.2 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: 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.16 \]](#)

2.20 192.168.0.142

Host scan start Sun May 5 04:44:45 2024 UTC
Host scan end Sun May 5 05:24:09 2024 UTC

Service (Port)	Threat Level
25/tcp	Medium
general/icmp	Low
22/tcp	Low

2.20.1 Medium 25/tcp

Medium (CVSS: 5.0)

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

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

Quality of Detection: 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

↔-----
TLShv1.0 | 10
TLShv1.1 | 10
TLShv1.2 | 10

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

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

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

Vulnerability Insight
... continues on next page ...

...continued from previous page ...
<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>> 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>
<p>Vulnerability Detection Method</p> <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: 2024-02-02T05:06:11Z</p>
<p>References</p> <p>cve: CVE-2011-1473</p> <p>cve: CVE-2011-5094</p> <p>url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/</p> <p>url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/</p> <p>url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation</p> <p>url: https://www.openwall.com/lists/oss-security/2011/07/08/2</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-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>
Medium (CVSS: 5.0)
NVT: Check if Mailserver answer to VRFY and EXPN requests
<p>Summary</p> <p>The Mailserver on this host answers to VRFY and/or EXPN requests.</p>
Quality of Detection: 99
<p>Vulnerability Detection Result</p> <p>'VRFY root' produces the following answer: 252 2.0.0 root</p>
... continues on next page ...

...continued from previous page ...
Solution: Solution type: Workaround Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.
Vulnerability Insight VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.
Vulnerability Detection Method Details: Check if Mailserver answer to VRFY and EXPN requests OID:1.3.6.1.4.1.25623.1.0.100072 Version used: 2023-10-31T05:06:37Z
References url: http://cr.yp.to/smtp/vrfy.html

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection: 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
... continues on next page ...

...continued from previous page ...
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
Affected Software/OS All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
Vulnerability Insight The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
Vulnerability Detection Method Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2023-10-20T16:09:12Z
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
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867

...continues on next page ...

...continued from previous page ...

```

dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482

```

[\[return to 192.168.0.142 \]](#)**2.20.2 Low general/icmp**

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary

The remote host responded to an ICMP timestamp request.

... continues on next page ...

...continued from previous page...	
Quality of Detection: 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: 2023-05-11T09:09:33Z	
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 dfn-cert: DFN-CERT-2014-0658	

[\[return to 192.168.0.142 \]](#)

2.20.3 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)
Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).
Quality of Detection: 80
Vulnerability Detection Result The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s): umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm ↪(s): umac-64-etm@openssh.com umac-64@openssh.com
Solution: Solution type: Mitigation Disable the reported weak MAC algorithm(s).
Vulnerability Detection Method Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[\[return to 192.168.0.142 \]](#)

2.21 192.168.0.5

Host scan start Sun May 5 03:01:04 2024 UTC
Host scan end Sun May 5 03:42:55 2024 UTC

Service (Port)	Threat Level
25/tcp	Medium
22/tcp	Low
general/icmp	Low

2.21.1 Medium 25/tcp

Medium (CVSS: 5.0)
NVT: Check if Mailserver answer to VRFY and EXPN requests
Summary The Mailserver on this host answers to VRFY and/or EXPN requests.
Quality of Detection: 99
Vulnerability Detection Result 'VRFY root' produces the following answer: 252 2.0.0 root
Solution: Solution type: Workaround Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.
Vulnerability Insight VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.
Vulnerability Detection Method Details: Check if Mailserver answer to VRFY and EXPN requests OID:1.3.6.1.4.1.25623.1.0.100072 Version used: 2023-10-31T05:06:37Z
References url: http://cr.yp.to/smtp/vrfy.html

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
...
... continues on next page ...

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

Medium (CVSS: 4.3)

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

Summary

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

Quality of Detection: 98

Vulnerability Detection Result

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

Impact

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

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

Solution:

Solution type: Mitigation

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

... continues on next page ...

...continued from previous page ...
Affected Software/OS All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
Vulnerability Insight The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
Vulnerability Detection Method Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2023-10-20T16:09:12Z
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-K13/0845 cert-bund: CB-K13/0796
...continues on next page ...

...continued from previous page ...	
cert-bund:	CB-K13/0790
dfn-cert:	DFN-CERT-2020-0177
dfn-cert:	DFN-CERT-2020-0111
dfn-cert:	DFN-CERT-2019-0068
dfn-cert:	DFN-CERT-2018-1441
dfn-cert:	DFN-CERT-2018-1408
dfn-cert:	DFN-CERT-2016-1372
dfn-cert:	DFN-CERT-2016-1164
dfn-cert:	DFN-CERT-2016-0388
dfn-cert:	DFN-CERT-2015-1853
dfn-cert:	DFN-CERT-2015-1332
dfn-cert:	DFN-CERT-2015-0884
dfn-cert:	DFN-CERT-2015-0800
dfn-cert:	DFN-CERT-2015-0758
dfn-cert:	DFN-CERT-2015-0567
dfn-cert:	DFN-CERT-2015-0544
dfn-cert:	DFN-CERT-2015-0530
dfn-cert:	DFN-CERT-2015-0396
dfn-cert:	DFN-CERT-2015-0375
dfn-cert:	DFN-CERT-2015-0374
dfn-cert:	DFN-CERT-2015-0305
dfn-cert:	DFN-CERT-2015-0199
dfn-cert:	DFN-CERT-2015-0079
dfn-cert:	DFN-CERT-2015-0021
dfn-cert:	DFN-CERT-2014-1414
dfn-cert:	DFN-CERT-2013-1847
dfn-cert:	DFN-CERT-2013-1792
dfn-cert:	DFN-CERT-2012-1979
dfn-cert:	DFN-CERT-2012-1829
dfn-cert:	DFN-CERT-2012-1530
dfn-cert:	DFN-CERT-2012-1380
dfn-cert:	DFN-CERT-2012-1377
dfn-cert:	DFN-CERT-2012-1292
dfn-cert:	DFN-CERT-2012-1214
dfn-cert:	DFN-CERT-2012-1213
dfn-cert:	DFN-CERT-2012-1180
dfn-cert:	DFN-CERT-2012-1156
dfn-cert:	DFN-CERT-2012-1155
dfn-cert:	DFN-CERT-2012-1039
dfn-cert:	DFN-CERT-2012-0956
dfn-cert:	DFN-CERT-2012-0908
dfn-cert:	DFN-CERT-2012-0868
dfn-cert:	DFN-CERT-2012-0867
dfn-cert:	DFN-CERT-2012-0848
dfn-cert:	DFN-CERT-2012-0838
dfn-cert:	DFN-CERT-2012-0776
dfn-cert:	DFN-CERT-2012-0722
...continues on next page ...	

...continued from previous page ...

```

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

```

[\[return to 192.168.0.5 \]](#)

2.21.2 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

The remote SSH server supports the following weak client-to-server MAC algorithm
...continues on next page ...

...continued from previous page ...
<pre> ↔(s): umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm ↔(s): umac-64-etm@openssh.com umac-64@openssh.com </pre>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>Disable the reported weak MAC algorithm(s).</p>
<p>Vulnerability Detection Method</p> <p>Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.</p> <p>Currently weak MAC algorithms are defined as the following:</p> <ul style="list-style-type: none"> - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm <p>Details: Weak MAC Algorithm(s) Supported (SSH)</p> <p>OID:1.3.6.1.4.1.25623.1.0.105610</p> <p>Version used: 2023-10-12T05:05:32Z</p>
<p>References</p> <p>url: https://www.rfc-editor.org/rfc/rfc6668</p> <p>url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4</p>

[[return to 192.168.0.5](#)]

2.21.3 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<p>Summary</p> <p>The remote host responded to an ICMP timestamp request.</p>
<p>Quality of Detection: 80</p>
<p>Vulnerability Detection Result</p> <p>The following response / ICMP packet has been received:</p> <ul style="list-style-type: none"> - ICMP Type: 14
... continues on next page ...

...continued from previous page...	
- 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: 2023-05-11T09:09:33Z	
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 dfn-cert: DFN-CERT-2014-0658	

[\[return to 192.168.0.5 \]](#)

2.22 192.168.0.141

Host scan start Sun May 5 04:51:03 2024 UTC

Host scan end Sun May 5 05:29:17 2024 UTC

Service (Port)	Threat Level
25/tcp	Medium
22/tcp	Low
general/icmp	Low

2.22.1 Medium 25/tcp

Medium (CVSS: 5.0)						
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)						
Summary The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.						
Quality of Detection: 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 ----- ↪----- <table><tr><td>TLSv1.0</td><td> 10</td></tr><tr><td>TLSv1.1</td><td> 10</td></tr><tr><td>TLSv1.2</td><td> 10</td></tr></table>	TLSv1.0	10	TLSv1.1	10	TLSv1.2	10
TLSv1.0	10					
TLSv1.1	10					
TLSv1.2	10					
Impact The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.						
Solution: Solution type: VendorFix Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.						
Affected Software/OS Every SSL/TLS service which does not properly restrict client-initiated renegotiation.						
Vulnerability Insight The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols. Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale: > It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment. Both CVEs are still kept in this VT as a reference to the origin of this flaw.						
Vulnerability Detection Method Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection. Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) OID:1.3.6.1.4.1.25623.1.0.117761 ... continues on next page ...						

...continued from previous page ...
Version used: 2024-02-02T05:06:11Z
References cve: CVE-2011-1473 cve: CVE-2011-5094 url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego-mitigation-dos/ url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/ url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation url: https://www.openwall.com/lists/oss-security/2011/07/08/2 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K17/0980 cert-bund: CB-K17/0979 cert-bund: CB-K13/0915 cert-bund: CB-K13/0462 dfn-cert: DFN-CERT-2017-1013 dfn-cert: DFN-CERT-2017-1012 dfn-cert: DFN-CERT-2014-0809 dfn-cert: DFN-CERT-2013-1928 dfn-cert: DFN-CERT-2012-1112

Medium (CVSS: 5.0)
NVT: Check if Mailserver answer to VRFY and EXPN requests
Summary The Mailserver on this host answers to VRFY and/or EXPN requests.
Quality of Detection: 99
Vulnerability Detection Result 'VRFY root' produces the following answer: 252 2.0.0 root
Solution: Solution type: Workaround Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.
Vulnerability Insight VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Details: Check if Mailserver answer to VRFY and EXPN requests OID:1.3.6.1.4.1.25623.1.0.100072 Version used: 2023-10-31T05:06:37Z
References url: http://cr.yp.to/smtp/vrfy.html

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection: 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: - 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)
... continues on next page ...

...continued from previous page ...

Vulnerability Detection Method

Check the used TLS protocols of the services provided by this system.

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

OID:1.3.6.1.4.1.25623.1.0.117274

Version used: 2023-10-20T16:09:12Z

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-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

...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

```

[\[return to 192.168.0.141 \]](#)

2.22.2 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

The remote SSH server supports the following weak client-to-server MAC algorithm \hookrightarrow (s):

umac-64-etm@openssh.com

umac-64@openssh.com

The remote SSH server supports the following weak server-to-client MAC algorithm \hookrightarrow (s):

umac-64-etm@openssh.com

umac-64@openssh.com

Solution:

... continues on next page ...

...continued from previous page ...
Solution type: Mitigation Disable the reported weak MAC algorithm(s).
Vulnerability Detection Method Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: <ul style="list-style-type: none"> - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[[return to 192.168.0.141](#)]

2.22.3 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: 80
Vulnerability Detection Result The following response / ICMP packet has been received: <ul style="list-style-type: none"> - 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:
... continues on next page ...

...continued from previous page ...

- 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: 2023-05-11T09:09:33Z

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

dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.141 \]](#)

2.23 192.168.0.9

Host scan start Sun May 5 03:48:38 2024 UTC

Host scan end Sun May 5 05:10:35 2024 UTC

Service (Port)	Threat Level
135/tcp	Medium
general/icmp	Low

2.23.1 Medium 135/tcp

Medium (CVSS: 5.0)

NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary

... continues on next page ...

...continued from previous page ...
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: 80
<p>Vulnerability Detection Result</p> <p>Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:</p> <p>Port: 49664/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:192.168.0.9[49664]</p> <p>Port: 49665/tcp UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:192.168.0.9[49665] Annotation: DHCP Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:192.168.0.9[49665] Annotation: DHCPv6 Client LRPC Endpoint UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:192.168.0.9[49665] Annotation: Event log TCPIP</p> <p>Port: 49668/tcp UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1 Endpoint: ncacn_ip_tcp:192.168.0.9[49668] Annotation: UserMgrCli UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1 Endpoint: ncacn_ip_tcp:192.168.0.9[49668] Annotation: AppInfo UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1 Endpoint: ncacn_ip_tcp:192.168.0.9[49668] UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1 Endpoint: ncacn_ip_tcp:192.168.0.9[49668] Annotation: Proxy Manager provider server endpoint UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1 Endpoint: ncacn_ip_tcp:192.168.0.9[49668] UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:192.168.0.9[49668] UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:192.168.0.9[49668] Annotation: IP Transition Configuration endpoint UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1 Endpoint: ncacn_ip_tcp:192.168.0.9[49668] Annotation: AppInfo UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1 Endpoint: ncacn_ip_tcp:192.168.0.9[49668] Annotation: AppInfo</p>
...continues on next page ...

...continued from previous page...	
UUID: 7d814569-35b3-4850-bb32-83035fcebfe, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49668]	
Annotation: IAS RPC server	
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49668]	
UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49668]	
Annotation: IKE/Authip API	
UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49668]	
Annotation: UserMgrCli	
UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49668]	
Annotation: Proxy Manager client server endpoint	
UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49668]	
Annotation: Adh APIs	
UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49668]	
Annotation: Impl friendly name	
UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49668]	
UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49668]	
Annotation: AppInfo	
UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49668]	
Annotation: AppInfo	
Port: 49669/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_ip_tcp:192.168.0.9[49669]	
Annotation: RemoteAccessCheck	
UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49669]	
Named pipe : lsass	
Win32 service or process : Netlogon	
Description : Net Logon service	
UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0	
Endpoint: ncacn_ip_tcp:192.168.0.9[49669]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : LSA access	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49669]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
...continues on next page...	

...continued from previous page...	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49669]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49669]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.9[49669]	
Annotation: KeyIso	
UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49669]	
Annotation: Impl friendly name	
UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4	
Endpoint: ncacn_ip_tcp:192.168.0.9[49669]	
Annotation: MS NT Directory DRS Interface	
UUID: f5cc5a18-4264-101a-8c59-08002b2f8426, version 56	
Endpoint: ncacn_ip_tcp:192.168.0.9[49669]	
Annotation: MS NT Directory NSP Interface	
Port: 49673/tcp	
UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49673]	
Annotation: Remote Fw APIs	
Port: 49674/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_http:192.168.0.9[49674]	
Annotation: RemoteAccessCheck	
UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1	
Endpoint: ncacn_http:192.168.0.9[49674]	
Named pipe : lsass	
Win32 service or process : Netlogon	
Description : Net Logon service	
UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0	
Endpoint: ncacn_http:192.168.0.9[49674]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : LSA access	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_http:192.168.0.9[49674]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_http:192.168.0.9[49674]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_http:192.168.0.9[49674]	
Annotation: Ngc Pop Key Service	
...continues on next page...	

...continued from previous page...	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_http:192.168.0.9[49674]	
Annotation: KeyIso	
UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4	
Endpoint: ncacn_http:192.168.0.9[49674]	
Annotation: MS NT Directory DRS Interface	
UUID: f5cc5a18-4264-101a-8c59-08002b2f8426, version 56	
Endpoint: ncacn_http:192.168.0.9[49674]	
Annotation: MS NT Directory NSP Interface	
Port: 49675/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_ip_tcp:192.168.0.9[49675]	
Annotation: RemoteAccessCheck	
UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49675]	
Named pipe : lsass	
Win32 service or process : Netlogon	
Description : Net Logon service	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49675]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49675]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[49675]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.9[49675]	
Annotation: KeyIso	
Port: 63420/tcp	
UUID: 0b6edbf4-4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[63420]	
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[63420]	
Named pipe : spoolss	
Win32 service or process : spoolsv.exe	
Description : Spooler service	
UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[63420]	
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[63420]	
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.9[63420]	
Port: 63439/tcp	
...continues on next page...	

...continued from previous page...	
UUID: a00c021c-2be2-11d2-b678-0000f87a8f8e, version 1 Endpoint: ncacn_ip_tcp:192.168.0.9[63439] Annotation: PERFMON SERVICE UUID: d049b186-814f-11d1-9a3c-00c04fc9b232, version 1 Endpoint: ncacn_ip_tcp:192.168.0.9[63439] Annotation: NtFrs API UUID: f5cc59b4-4264-101a-8c59-08002b2f8426, version 1 Endpoint: ncacn_ip_tcp:192.168.0.9[63439] Annotation: NtFrs Service Port: 63503/tcp UUID: 91ae6020-9e3c-11cf-8d7c-00aa00c091be, version 0 Endpoint: ncacn_ip_tcp:192.168.0.9[63503] Named pipe : cert Win32 service or process : certsrv.exe Description : Certificate service Port: 63505/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:192.168.0.9[63505] Port: 63641/tcp UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5 Endpoint: ncacn_ip_tcp:192.168.0.9[63641] Named pipe : dnsserver Win32 service or process : dns.exe Description : DNS Server 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.	
Impact	An attacker may use this fact to gain more knowledge about the remote host.
Solution:	
Solution type: Mitigation	Filter incoming traffic to this ports.
Vulnerability Detection Method	
Details: DCE/RPC and MSRPC Services Enumeration Reporting	
OID:1.3.6.1.4.1.25623.1.0.10736	
Version used: 2022-06-03T10:17:07Z	

[\[return to 192.168.0.9 \]](#)

2.23.2 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: 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.9 \]](#)

2.24 192.168.0.209

Host scan start Sun May 5 04:17:13 2024 UTC

Host scan end Sun May 5 05:25:25 2024 UTC

Service (Port)	Threat Level
443/tcp	Medium
general/icmp	Low
22/tcp	Low

2.24.1 Medium 443/tcp

Medium (CVSS: 5.0)

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

Summary

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

Quality of Detection: 99**Vulnerability Detection Result**

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

Issuer: CN=localhost

Certificate details:

fingerprint (SHA-1)	764E4AB0FE870E64B76C87B7290D6B3978E61913
fingerprint (SHA-256)	65BEF221DA2786DA4DAA0CF6A080835C15B8B0237A9697
↪3FEE29A5157CD360D7	
issued by	CN=localhost
public key algorithm	RSA
public key size (bits)	4096
serial	66E22F5208019400DC02A5E7794738A153D3B850
signature algorithm	sha256WithRSAEncryption
subject	CN=localhost
subject alternative names (SAN)	None
valid from	2023-11-29 12:18:33 UTC
valid until	2024-11-28 12:18:33 UTC

Impact

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

Solution:**Solution type:** Mitigation

... continues on next page ...

...continued from previous page ...
Replace the SSL/TLS certificate with one signed by a trusted CA.
Vulnerability Detection Method The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA. Details: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection OID:1.3.6.1.4.1.25623.1.0.113054 Version used: 2021-11-22T15:32:39Z

[\[return to 192.168.0.209 \]](#)

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: 80
Vulnerability Detection Result The following response / ICMP packet has been received: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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.
... 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: 2023-05-11T09:09:33Z

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

dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.209 \]](#)

2.24.3 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

The remote SSH server supports the following weak client-to-server MAC algorithm \hookrightarrow (s):

umac-64-etm@openssh.com

umac-64@openssh.com

The remote SSH server supports the following weak server-to-client MAC algorithm \hookrightarrow (s):

umac-64-etm@openssh.com

umac-64@openssh.com

Solution:

Solution type: Mitigation

Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method

Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.

... continues on next page ...

...continued from previous page ...
Currently weak MAC algorithms are defined as the following: <ul style="list-style-type: none">- MD5 based algorithms- 96-bit based algorithms- 64-bit based algorithms- 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[\[return to 192.168.0.209 \]](#)

2.25 192.168.0.106

Host scan start Sun May 5 03:01:04 2024 UTC
Host scan end Sun May 5 04:44:44 2024 UTC

Service (Port)	Threat Level
135/tcp	Medium
general/icmp	Low

2.25.1 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: 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: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:192.168.0.106[49664] Port: 49665/tcp
... continues on next page ...

...continued from previous page...	
UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49665]	
Annotation: DHCP Client LRPC Endpoint	
UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49665]	
Annotation: DHCPv6 Client LRPC Endpoint	
UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49665]	
Annotation: Event log TCPIP	
Port: 49668/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_ip_tcp:192.168.0.106[49668]	
Annotation: RemoteAccessCheck	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49668]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : SAM access	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49668]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49668]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.106[49668]	
Annotation: KeyIso	
Port: 49669/tcp	
UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49669]	
Annotation: UserMgrCli	
UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49669]	
Annotation: AppInfo	
UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49669]	
UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49669]	
Annotation: Proxy Manager provider server endpoint	
UUID: 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.106[49669]	
UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49669]	
UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49669]	
Annotation: IP Transition Configuration endpoint	
UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1	
...continues on next page...	

...continued from previous page...	
Endpoint: ncacn_ip_tcp:192.168.0.106[49669]	
Annotation: AppInfo	
UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49669]	
Annotation: AppInfo	
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49669]	
UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49669]	
Annotation: IKE/Authip API	
UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49669]	
Annotation: UserMgrCli	
UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49669]	
Annotation: Proxy Manager client server endpoint	
UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49669]	
Annotation: Adh APIs	
UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49669]	
Annotation: AppInfo	
UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49669]	
Annotation: AppInfo	
Port: 49687/tcp	
UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49687]	
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49687]	
Named pipe : spoolss	
Win32 service or process : spoolsv.exe	
Description : Spooler service	
UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49687]	
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49687]	
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49687]	
Port: 49699/tcp	
UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.106[49699]	
Annotation: Remote Fw APIs	
Port: 49705/tcp	
UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4	
Endpoint: ncacn_ip_tcp:192.168.0.106[49705]	
Annotation: 389	
...continues on next page...	

...continued from previous page ...
Port: 49713/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:192.168.0.106[49713] Port: 62155/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:192.168.0.106[62155] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access 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.
Impact An attacker may use this fact to gain more knowledge about the remote host.
Solution: Solution type: Mitigation Filter incoming traffic to this ports.
Vulnerability Detection Method Details: DCE/RPC and MSRPC Services Enumeration Reporting OID:1.3.6.1.4.1.25623.1.0.10736 Version used: 2022-06-03T10:17:07Z

[\[return to 192.168.0.106 \]](#)

2.25.2 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: 80
Vulnerability Detection Result The following response / ICMP packet has been received: <ul style="list-style-type: none"> - ICMP Type: 14 - ICMP Code: 0
Impact ... 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: 2023-05-11T09:09:33Z

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

dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.106 \]](#)

2.26 192.168.0.57

Host scan start Sun May 5 04:45:55 2024 UTC

Host scan end Sun May 5 05:37:04 2024 UTC

Service (Port)	Threat Level
80/tcp	Medium
25/tcp	Medium
22/tcp	Low
general/icmp	Low

2.26.1 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP
Summary The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.
Quality of Detection: 80
Vulnerability Detection Result The following URLs requires Basic Authentication (URL:realm name): http://dspam.compwire.local/dspam:"DSPAM Control Center"
Impact An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.
Solution: Solution type: Workaround Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.
Affected Software/OS Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.
Vulnerability Detection Method Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection. The script is currently checking the following: - HTTP Basic Authentication (Basic Auth) - HTTP Forms (e.g. Login) with input field of type 'password' Details: Cleartext Transmission of Sensitive Information via HTTP OID:1.3.6.1.4.1.25623.1.0.108440 Version used: 2023-09-07T05:05:21Z
References url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure url: https://cwe.mitre.org/data/definitions/319.html

[\[return to 192.168.0.57 \]](#)

2.26.2 Medium 25/tcp

Medium (CVSS: 5.0)																															
NVT: SSL/TLS: Certificate Expired																															
Summary The remote server's SSL/TLS certificate has already expired.																															
Quality of Detection: 99																															
Vulnerability Detection Result The certificate of the remote service expired on 2021-08-20 22:05:28. Certificate details: <table> <tr> <td>fingerprint (SHA-1)</td><td> 0733ED753BE245B3F339F6913690A3201C5E8E64</td></tr> <tr> <td>fingerprint (SHA-256)</td><td> 2E9520D72F81B5A79720E2B8FF1DBD97CF1ED3FAD10BB9</td></tr> <tr> <td>↪922ACC7EE07145CE84</td><td></td></tr> <tr> <td>issued by</td><td> CN=Go Daddy Secure Certificate Authority - G2,</td></tr> <tr> <td>↪OU=http://certs.godaddy.com/repository/,O=GoDaddy.com\, Inc.,L=Scottsdale,ST=A</td><td></td></tr> <tr> <td>↪rizona,C=US</td><td></td></tr> <tr> <td>public key algorithm</td><td> RSA</td></tr> <tr> <td>public key size (bits)</td><td> 2048</td></tr> <tr> <td>serial</td><td> 00B529AE3A68E919AE</td></tr> <tr> <td>signature algorithm</td><td> sha256WithRSAEncryption</td></tr> <tr> <td>subject</td><td> CN=*.compwire.com.br,OU=Domain Control Validat</td></tr> <tr> <td>↪ed</td><td></td></tr> <tr> <td>subject alternative names (SAN)</td><td> *.compwire.com.br, compwire.com.br</td></tr> <tr> <td>valid from</td><td> 2019-08-20 22:05:28 UTC</td></tr> <tr> <td>valid until</td><td> 2021-08-20 22:05:28 UTC</td></tr> </table>		fingerprint (SHA-1)	0733ED753BE245B3F339F6913690A3201C5E8E64	fingerprint (SHA-256)	2E9520D72F81B5A79720E2B8FF1DBD97CF1ED3FAD10BB9	↪922ACC7EE07145CE84		issued by	CN=Go Daddy Secure Certificate Authority - G2,	↪OU=http://certs.godaddy.com/repository/,O=GoDaddy.com\, Inc.,L=Scottsdale,ST=A		↪rizona,C=US		public key algorithm	RSA	public key size (bits)	2048	serial	00B529AE3A68E919AE	signature algorithm	sha256WithRSAEncryption	subject	CN=*.compwire.com.br,OU=Domain Control Validat	↪ed		subject alternative names (SAN)	*.compwire.com.br, compwire.com.br	valid from	2019-08-20 22:05:28 UTC	valid until	2021-08-20 22:05:28 UTC
fingerprint (SHA-1)	0733ED753BE245B3F339F6913690A3201C5E8E64																														
fingerprint (SHA-256)	2E9520D72F81B5A79720E2B8FF1DBD97CF1ED3FAD10BB9																														
↪922ACC7EE07145CE84																															
issued by	CN=Go Daddy Secure Certificate Authority - G2,																														
↪OU=http://certs.godaddy.com/repository/,O=GoDaddy.com\, Inc.,L=Scottsdale,ST=A																															
↪rizona,C=US																															
public key algorithm	RSA																														
public key size (bits)	2048																														
serial	00B529AE3A68E919AE																														
signature algorithm	sha256WithRSAEncryption																														
subject	CN=*.compwire.com.br,OU=Domain Control Validat																														
↪ed																															
subject alternative names (SAN)	*.compwire.com.br, compwire.com.br																														
valid from	2019-08-20 22:05:28 UTC																														
valid until	2021-08-20 22:05:28 UTC																														
Solution: Solution type: Mitigation Replace the SSL/TLS certificate by a new one.																															
Vulnerability Insight This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.																															
Vulnerability Detection Method Details: SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: 2021-11-22T15:32:39Z																															

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: 70
Vulnerability Detection Result The following indicates that the remote SSL/TLS service is affected: Protocol Version Successful re-done SSL/TLS handshakes (Renegotiation) over an ↪ existing / already established SSL/TLS connection ----- ↪----- TLSv1.0 10 TLSv1.1 10 TLSv1.2 10
Impact The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.
Solution: Solution type: VendorFix Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.
Affected Software/OS Every SSL/TLS service which does not properly restrict client-initiated renegotiation.
Vulnerability Insight The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols. Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale: > It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment. Both CVEs are still kept in this VT as a reference to the origin of this flaw.
Vulnerability Detection Method Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection. Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) OID:1.3.6.1.4.1.25623.1.0.117761 ... continues on next page ...

...continued from previous page ...
Version used: 2024-02-02T05:06:11Z
References cve: CVE-2011-1473 cve: CVE-2011-5094 url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego-mitiation-dos/ url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/ url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation url: https://www.openwall.com/lists/oss-security/2011/07/08/2 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K17/0980 cert-bund: CB-K17/0979 cert-bund: CB-K13/0915 cert-bund: CB-K13/0462 dfn-cert: DFN-CERT-2017-1013 dfn-cert: DFN-CERT-2017-1012 dfn-cert: DFN-CERT-2014-0809 dfn-cert: DFN-CERT-2013-1928 dfn-cert: DFN-CERT-2012-1112

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection: 98
Vulnerability Detection Result In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
Impact An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.
Solution: Solution type: Mitigation
... continues on next page ...

...continued from previous page ...
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
Affected Software/OS All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
Vulnerability Insight The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
Vulnerability Detection Method Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2023-10-20T16:09:12Z
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
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867

...continues on next page ...

...continued from previous page ...

```

dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482

```

[\[return to 192.168.0.57 \]](#)**2.26.3 Low 22/tcp**

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary

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

... continues on next page ...

...continued from previous page ...
Quality of Detection: 80
Vulnerability Detection Result The remote SSH server supports the following weak client-to-server MAC algorithm $\hookrightarrow(s)$: umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm $\hookrightarrow(s)$: umac-64-etm@openssh.com umac-64@openssh.com
Solution: Solution type: Mitigation Disable the reported weak MAC algorithm(s).
Vulnerability Detection Method Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[[return to 192.168.0.57](#)]

2.26.4 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: 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: 2023-05-11T09:09:33Z

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

dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.57 \]](#)

2.27 192.168.0.28

Host scan start Sun May 5 03:29:04 2024 UTC

Host scan end Sun May 5 04:10:04 2024 UTC

Service (Port)	Threat Level
25/tcp	Medium

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
22/tcp	Low
general/icmp	Low

2.27.1 Medium 25/tcp

Medium (CVSS: 5.0)

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

Summary

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

Quality of Detection: 70

Vulnerability Detection Result

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

 ↔-----
 TLSv1.0 | 10
 TLSv1.1 | 10
 TLSv1.2 | 10

Impact

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

Solution:

Solution type: VendorFix

Users should contact their vendors for specific patch information.

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

Affected Software/OS

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

Vulnerability Insight

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

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

... continues on next page ...

...continued from previous page ...
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment. Both CVEs are still kept in this VT as a reference to the origin of this flaw.
Vulnerability Detection Method Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection. Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) OID:1.3.6.1.4.1.25623.1.0.117761 Version used: 2024-02-02T05:06:11Z
References cve: CVE-2011-1473 cve: CVE-2011-5094 url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/ url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/ url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation url: https://www.openwall.com/lists/oss-security/2011/07/08/2 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K17/0980 cert-bund: CB-K17/0979 cert-bund: CB-K13/0915 cert-bund: CB-K13/0462 dfn-cert: DFN-CERT-2017-1013 dfn-cert: DFN-CERT-2017-1012 dfn-cert: DFN-CERT-2014-0809 dfn-cert: DFN-CERT-2013-1928 dfn-cert: DFN-CERT-2012-1112
Medium (CVSS: 5.0)
NVT: Check if Mailserver answer to VRFY and EXPN requests
Summary The Mailserver on this host answers to VRFY and/or EXPN requests.
Quality of Detection: 99
Vulnerability Detection Result 'VRFY root' produces the following answer: 252 2.0.0 root
Solution: Solution type: Workaround Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. ... continues on next page ...

...continued from previous page ...
<p>For Sendmail add the option 'O PrivacyOptions=goaway'.</p> <p>It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.</p>
<p>Vulnerability Insight</p> <p>VERFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.</p>
<p>Vulnerability Detection Method</p> <p>Details: Check if Mailserver answer to VRFY and EXPN requests</p> <p>OID:1.3.6.1.4.1.25623.1.0.100072</p> <p>Version used: 2023-10-31T05:06:37Z</p>
<p>References</p> <p>url: http://cr.yp.to/smtp/vrfy.html</p>

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
<p>Summary</p> <p>It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.</p>
<p>Quality of Detection: 98</p>
<p>Vulnerability Detection Result</p> <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>Impact</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>Solution:</p> <p>Solution type: 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>
... continues on next page ...

...continued from previous page ...
Affected Software/OS All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
Vulnerability Insight The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
Vulnerability Detection Method Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2023-10-20T16:09:12Z
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-K13/0845 cert-bund: CB-K13/0796
...continues on next page ...

...continued from previous page ...	
cert-bund:	CB-K13/0790
dfn-cert:	DFN-CERT-2020-0177
dfn-cert:	DFN-CERT-2020-0111
dfn-cert:	DFN-CERT-2019-0068
dfn-cert:	DFN-CERT-2018-1441
dfn-cert:	DFN-CERT-2018-1408
dfn-cert:	DFN-CERT-2016-1372
dfn-cert:	DFN-CERT-2016-1164
dfn-cert:	DFN-CERT-2016-0388
dfn-cert:	DFN-CERT-2015-1853
dfn-cert:	DFN-CERT-2015-1332
dfn-cert:	DFN-CERT-2015-0884
dfn-cert:	DFN-CERT-2015-0800
dfn-cert:	DFN-CERT-2015-0758
dfn-cert:	DFN-CERT-2015-0567
dfn-cert:	DFN-CERT-2015-0544
dfn-cert:	DFN-CERT-2015-0530
dfn-cert:	DFN-CERT-2015-0396
dfn-cert:	DFN-CERT-2015-0375
dfn-cert:	DFN-CERT-2015-0374
dfn-cert:	DFN-CERT-2015-0305
dfn-cert:	DFN-CERT-2015-0199
dfn-cert:	DFN-CERT-2015-0079
dfn-cert:	DFN-CERT-2015-0021
dfn-cert:	DFN-CERT-2014-1414
dfn-cert:	DFN-CERT-2013-1847
dfn-cert:	DFN-CERT-2013-1792
dfn-cert:	DFN-CERT-2012-1979
dfn-cert:	DFN-CERT-2012-1829
dfn-cert:	DFN-CERT-2012-1530
dfn-cert:	DFN-CERT-2012-1380
dfn-cert:	DFN-CERT-2012-1377
dfn-cert:	DFN-CERT-2012-1292
dfn-cert:	DFN-CERT-2012-1214
dfn-cert:	DFN-CERT-2012-1213
dfn-cert:	DFN-CERT-2012-1180
dfn-cert:	DFN-CERT-2012-1156
dfn-cert:	DFN-CERT-2012-1155
dfn-cert:	DFN-CERT-2012-1039
dfn-cert:	DFN-CERT-2012-0956
dfn-cert:	DFN-CERT-2012-0908
dfn-cert:	DFN-CERT-2012-0868
dfn-cert:	DFN-CERT-2012-0867
dfn-cert:	DFN-CERT-2012-0848
dfn-cert:	DFN-CERT-2012-0838
dfn-cert:	DFN-CERT-2012-0776
dfn-cert:	DFN-CERT-2012-0722
...continues on next page ...	

...continued from previous page ...

```

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

```

[\[return to 192.168.0.28 \]](#)

2.27.2 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

The remote SSH server supports the following weak client-to-server MAC algorithm
...continues on next page ...

...continued from previous page ...
<pre> ↔(s): umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm ↔(s): umac-64-etm@openssh.com umac-64@openssh.com </pre>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>Disable the reported weak MAC algorithm(s).</p>
<p>Vulnerability Detection Method</p> <p>Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.</p> <p>Currently weak MAC algorithms are defined as the following:</p> <ul style="list-style-type: none"> - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm <p>Details: Weak MAC Algorithm(s) Supported (SSH)</p> <p>OID:1.3.6.1.4.1.25623.1.0.105610</p> <p>Version used: 2023-10-12T05:05:32Z</p>
<p>References</p> <p>url: https://www.rfc-editor.org/rfc/rfc6668</p> <p>url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4</p>

[[return to 192.168.0.28](#)]

2.27.3 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<p>Summary</p> <p>The remote host responded to an ICMP timestamp request.</p>
<p>Quality of Detection: 80</p>
<p>Vulnerability Detection Result</p> <p>The following response / ICMP packet has been received:</p> <ul style="list-style-type: none"> - ICMP Type: 14
...continues on next page ...

...continued from previous page ...	
- 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: 2023-05-11T09:09:33Z	
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 dfn-cert: DFN-CERT-2014-0658	

[\[return to 192.168.0.28 \]](#)

2.28 192.168.0.99

Host scan start Sun May 5 03:56:35 2024 UTC

Host scan end Sun May 5 05:44:13 2024 UTC

Service (Port)	Threat Level
135/tcp	Medium
general/icmp	Low

2.28.1 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: 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: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
Endpoint: ncacn_ip_tcp:192.168.0.99[49664]

Port: 49665/tcp

UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
Endpoint: ncacn_ip_tcp:192.168.0.99[49665]

Annotation: DHCP Client LRPC Endpoint

UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
Endpoint: ncacn_ip_tcp:192.168.0.99[49665]

Annotation: DHCPv6 Client LRPC Endpoint

UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
Endpoint: ncacn_ip_tcp:192.168.0.99[49665]

Annotation: Event log TCPIP

Port: 49667/tcp

UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
Endpoint: ncacn_ip_tcp:192.168.0.99[49667]

Annotation: RemoteAccessCheck

UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
Endpoint: ncacn_ip_tcp:192.168.0.99[49667]

Named pipe : lsass

Win32 service or process : lsass.exe

Description : SAM access

UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
Endpoint: ncacn_ip_tcp:192.168.0.99[49667]

Annotation: Ngc Pop Key Service

UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
Endpoint: ncacn_ip_tcp:192.168.0.99[49667]

Annotation: Ngc Pop Key Service

UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
Endpoint: ncacn_ip_tcp:192.168.0.99[49667]

Annotation: KeyIso

Port: 49669/tcp

UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]

... continues on next page ...

...continued from previous page...	
Annotation: UserMgrCli	
UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]	
Annotation: AppInfo	
UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]	
UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]	
Annotation: Proxy Manager provider server endpoint	
UUID: 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]	
UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]	
UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]	
Annotation: IP Transition Configuration endpoint	
UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]	
Annotation: AppInfo	
UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]	
Annotation: AppInfo	
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]	
UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]	
Annotation: IKE/Authip API	
UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]	
Annotation: UserMgrCli	
UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]	
Annotation: Proxy Manager client server endpoint	
UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]	
Annotation: Adh APIs	
UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]	
UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]	
Annotation: AppInfo	
UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.99[49669]	
Annotation: AppInfo	
Port: 49674/tcp	
UUID: 0b6edbf-a4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.99[49674]	
...continues on next page...	

...continued from previous page...	
<pre> UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:192.168.0.99[49674] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:192.168.0.99[49674] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:192.168.0.99[49674] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:192.168.0.99[49674] Port: 49702/tcp UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1 Endpoint: ncacn_ip_tcp:192.168.0.99[49702] Annotation: Remote Fw APIs Port: 49713/tcp UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4 Endpoint: ncacn_ip_tcp:192.168.0.99[49713] Annotation: 389 Port: 49715/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:192.168.0.99[49715] Port: 55178/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:192.168.0.99[55178] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access 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>	
Impact	An attacker may use this fact to gain more knowledge about the remote host.
Solution:	
Solution type: Mitigation	Filter incoming traffic to this ports.
Vulnerability Detection Method	
Details: DCE/RPC and MSRPC Services Enumeration Reporting OID:1.3.6.1.4.1.25623.1.0.10736 Version used: 2022-06-03T10:17:07Z	

[\[return to 192.168.0.99 \]](#)

2.28.2 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: 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.99 \]](#)

2.29 192.168.0.25

Host scan start Sun May 5 03:45:14 2024 UTC

Host scan end Sun May 5 04:59:19 2024 UTC

Service (Port)	Threat Level
3389/tcp	Medium
135/tcp	Medium
general/icmp	Low

2.29.1 Medium 3389/tcp

Medium (CVSS: 4.3)

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

Summary

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

Quality of Detection: 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"> - 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. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2023-10-20T16:09:12Z</p>
<p>References</p> <p>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-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</p>
...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

```

[\[return to 192.168.0.25 \]](#)

2.29.2 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: 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

...continues on next page ...

...continued from previous page...	
Endpoint: ncacn_ip_tcp:192.168.0.25[49664]	
Annotation: RemoteAccessCheck	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.25[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:192.168.0.25[49664]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.25[49664]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.25[49664]	
Annotation: KeyIso	
Port: 49665/tcp	
UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.25[49665]	
Port: 49666/tcp	
UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.25[49666]	
Annotation: Event log TCPIP	
Port: 49667/tcp	
UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.25[49667]	
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.25[49667]	
Port: 49669/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_ip_tcp:192.168.0.25[49669]	
Annotation: RemoteAccessCheck	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.25[49669]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.25[49669]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.0.25[49669]	
Annotation: KeyIso	
Port: 49670/tcp	
UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.25[49670]	
Port: 49674/tcp	
UUID: 0b6edbf-a4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.0.25[49674]	
...continues on next page...	

<p>...continued from previous page ...</p> <p>UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:192.168.0.25[49674] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:192.168.0.25[49674] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:192.168.0.25[49674] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:192.168.0.25[49674] Port: 49701/tcp UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1 Endpoint: ncacn_ip_tcp:192.168.0.25[49701] Annotation: Remote Fw APIs Port: 49705/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:192.168.0.25[49705] 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.</p>
<p>Impact An attacker may use this fact to gain more knowledge about the remote host.</p>
<p>Solution: Solution type: Mitigation Filter incoming traffic to this ports.</p>
<p>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</p>

[\[return to 192.168.0.25 \]](#)

2.29.3 Low general/icmp

<p>Low (CVSS: 2.1)</p> <p>NVT: ICMP Timestamp Reply Information Disclosure</p>
<p>Summary The remote host responded to an ICMP timestamp request.</p>
<p>... continues on next page ...</p>

...continued from previous page...
Quality of Detection: 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.25 \]](#)

2.30 192.168.0.104

Host scan start Sun May 5 03:01:04 2024 UTC
Host scan end Sun May 5 03:40:51 2024 UTC

Service (Port)	Threat Level
25/tcp	Medium
22/tcp	Low
general/icmp	Low

2.30.1 Medium 25/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
Summary The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.
Quality of Detection: 70
Vulnerability Detection Result The following indicates that the remote SSL/TLS service is affected: Protocol Version Successful re-done SSL/TLS handshakes (Renegotiation) over an ↪ existing / already established SSL/TLS connection ----- ↪----- TLSv1.0 10 TLSv1.1 10 TLSv1.2 10
Impact The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.
Solution: Solution type: VendorFix Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.
Affected Software/OS Every SSL/TLS service which does not properly restrict client-initiated renegotiation.
Vulnerability Insight The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols. Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale: ... continues on next page ...

...continued from previous page ...
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment. Both CVEs are still kept in this VT as a reference to the origin of this flaw.
Vulnerability Detection Method Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection. Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) OID:1.3.6.1.4.1.25623.1.0.117761 Version used: 2024-02-02T05:06:11Z
References cve: CVE-2011-1473 cve: CVE-2011-5094 url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/ url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/ url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation url: https://www.openwall.com/lists/oss-security/2011/07/08/2 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K17/0980 cert-bund: CB-K17/0979 cert-bund: CB-K13/0915 cert-bund: CB-K13/0462 dfn-cert: DFN-CERT-2017-1013 dfn-cert: DFN-CERT-2017-1012 dfn-cert: DFN-CERT-2014-0809 dfn-cert: DFN-CERT-2013-1928 dfn-cert: DFN-CERT-2012-1112
Medium (CVSS: 5.0)
NVT: Check if Mailserver answer to VRFY and EXPN requests
Summary The Mailserver on this host answers to VRFY and/or EXPN requests.
Quality of Detection: 99
Vulnerability Detection Result 'VRFY root' produces the following answer: 550 5.7.1 <root>: Recipient address rejected: Please see http://www.openspf.org/Why?s=helo;id=example.com;ip=192.168.42.88;r=smtp1.compwire.local
Solution: Solution type: Workaround
... continues on next page ...

...continued from previous page ...
<p>Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.</p>
<p>Vulnerability Insight VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.</p>
<p>Vulnerability Detection Method Details: Check if Mailserver answer to VRFY and EXPN requests OID:1.3.6.1.4.1.25623.1.0.100072 Version used: 2023-10-31T05:06:37Z</p>
<p>References url: http://cr.yp.to/smtp/vrfy.html</p>

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
<p>Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.</p>
<p>Quality of Detection: 98</p>
<p>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.</p>
<p>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.</p>
<p>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.</p>
... continues on next page ...

...continued from previous page ...
Affected Software/OS All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
Vulnerability Insight The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
Vulnerability Detection Method Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2023-10-20T16:09:12Z
References cve: CVE-2011-3389 cve: CVE-2015-0204 url: https://ssl-config.mozilla.org/ url: https://bettercrypto.org/ url: https://datatracker.ietf.org/doc/rfc8996/ url: https://vnhacker.blogspot.com/2011/09/beast.html url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters ↔-report-2014 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K18/0799 cert-bund: CB-K16/1289 cert-bund: CB-K16/1096 cert-bund: CB-K15/1751 cert-bund: CB-K15/1266 cert-bund: CB-K15/0850 cert-bund: CB-K15/0764 cert-bund: CB-K15/0720 cert-bund: CB-K15/0548 cert-bund: CB-K15/0526 cert-bund: CB-K15/0509 cert-bund: CB-K15/0493 cert-bund: CB-K15/0384 cert-bund: CB-K15/0365 cert-bund: CB-K15/0364 cert-bund: CB-K15/0302 cert-bund: CB-K15/0192 cert-bund: CB-K15/0079 cert-bund: CB-K15/0016
...continues on next page ...

...continued from previous page ...

cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838

...continues on next page ...

...continued from previous page ...

```

dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482

```

[\[return to 192.168.0.104 \]](#)

2.30.2 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary

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

Quality of Detection: 80

...continues on next page ...

...continued from previous page ...
Vulnerability Detection Result The remote SSH server supports the following weak client-to-server MAC algorithm $\hookrightarrow(s)$: umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm $\hookleftarrow(s)$: umac-64-etm@openssh.com umac-64@openssh.com
Solution: Solution type: Mitigation Disable the reported weak MAC algorithm(s).
Vulnerability Detection Method Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[[return to 192.168.0.104](#)]

2.30.3 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: 80
Vulnerability Detection Result ... continues on next page ...

...continued from previous page...
<p>The following response / ICMP packet has been received:</p> <ul style="list-style-type: none"> - ICMP Type: 14 - ICMP Code: 0
<p>Impact</p> <p>This information could theoretically be used to exploit weak time-based random number generators in other services.</p>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>Various mitigations are possible:</p> <ul style="list-style-type: none"> - 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)
<p>Vulnerability Insight</p> <p>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.</p>
<p>Vulnerability Detection Method</p> <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: 2023-05-11T09:09:33Z</p>
<p>References</p> <p>cve: CVE-1999-0524</p> <p>url: https://datatracker.ietf.org/doc/html/rfc792</p> <p>url: https://datatracker.ietf.org/doc/html/rfc2780</p> <p>cert-bund: CB-K15/1514</p> <p>dfn-cert: DFN-CERT-2014-0658</p>

[\[return to 192.168.0.104 \]](#)

2.31 192.168.0.246

Host scan start Sun May 5 03:31:33 2024 UTC
Host scan end Sun May 5 04:24:26 2024 UTC

Service (Port)	Threat Level
80/tcp	Medium
general/icmp	Low
22/tcp	Low

2.31.1 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP
Summary The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.
Quality of Detection: 80
Vulnerability Detection Result The following input fields were identified (URL:input name): http://srvzabbixcpw.compwire.local/:password
Impact An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.
Solution: Solution type: Workaround Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.
Affected Software/OS Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.
Vulnerability Detection Method Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection. The script is currently checking the following: - HTTP Basic Authentication (Basic Auth) - HTTP Forms (e.g. Login) with input field of type 'password' Details: Cleartext Transmission of Sensitive Information via HTTP OID:1.3.6.1.4.1.25623.1.0.108440 Version used: 2023-09-07T05:05:21Z
References url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure url: https://cwe.mitre.org/data/definitions/319.html

[\[return to 192.168.0.246 \]](#)

2.31.2 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: 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: 2023-05-11T09:09:33Z
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
... continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.246 \]](#)**2.31.3 Low 22/tcp**

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary

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

Quality of Detection: 80**Vulnerability Detection Result**The remote SSH server supports the following weak client-to-server MAC algorithm
↔(s):

umac-64-etm@openssh.com

umac-64@openssh.com

The remote SSH server supports the following weak server-to-client MAC algorithm
↔(s):

umac-64-etm@openssh.com

umac-64@openssh.com

Solution:**Solution type:** Mitigation

Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method

Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.

Currently weak MAC algorithms are defined as the following:

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

Details: Weak MAC Algorithm(s) Supported (SSH)

OID:1.3.6.1.4.1.25623.1.0.105610

Version used: 2023-10-12T05:05:32Z

Referencesurl: <https://www.rfc-editor.org/rfc/rfc6668>url: <https://www.rfc-editor.org/rfc/rfc4253#section-6.4>

[\[return to 192.168.0.246 \]](#)

2.32 192.168.0.130

Host scan start Sun May 5 03:01:04 2024 UTC

Host scan end Sun May 5 03:46:03 2024 UTC

Service (Port)	Threat Level
80/tcp	Medium
22/tcp	Low
general/icmp	Low

2.32.1 Medium 80/tcp

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

The following input fields were identified (URL:input name):

<http://192.168.0.130/:password>

Impact

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

Solution:

Solution type: Workaround

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

Affected Software/OS

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

Vulnerability Detection Method

... continues on next page ...

...continued from previous page...
<p>Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.</p> <p>The script is currently checking the following:</p> <ul style="list-style-type: none"> - HTTP Basic Authentication (Basic Auth) - HTTP Forms (e.g. Login) with input field of type 'password' <p>Details: Cleartext Transmission of Sensitive Information via HTTP</p> <p>OID:1.3.6.1.4.1.25623.1.0.108440</p> <p>Version used: 2023-09-07T05:05:21Z</p>
<p>References</p> <p>url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management</p> <p>url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure</p> <p>url: https://cwe.mitre.org/data/definitions/319.html</p>

[[return to 192.168.0.130](#)]

2.32.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)
<p>Summary</p> <p>The remote SSH server is configured to allow / support weak MAC algorithm(s).</p>
Quality of Detection: 80
<p>Vulnerability Detection Result</p> <p>The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s):</p> <p>umac-64-etm@openssh.com</p> <p>umac-64@openssh.com</p> <p>The remote SSH server supports the following weak server-to-client MAC algorithm ↪(s):</p> <p>umac-64-etm@openssh.com</p> <p>umac-64@openssh.com</p>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>Disable the reported weak MAC algorithm(s).</p>
Vulnerability Detection Method
... continues on next page ...

...continued from previous page ...
<p>Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.</p> <p>Currently weak MAC algorithms are defined as the following:</p> <ul style="list-style-type: none"> - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm <p>Details: Weak MAC Algorithm(s) Supported (SSH)</p> <p>OID:1.3.6.1.4.1.25623.1.0.105610</p> <p>Version used: 2023-10-12T05:05:32Z</p>
<p>References</p> <p>url: https://www.rfc-editor.org/rfc/rfc6668</p> <p>url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4</p>

[[return to 192.168.0.130](#)]

2.32.3 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<p>Summary</p> <p>The remote host responded to an ICMP timestamp request.</p>
<p>Quality of Detection: 80</p>
<p>Vulnerability Detection Result</p> <p>The following response / ICMP packet has been received:</p> <ul style="list-style-type: none"> - ICMP Type: 14 - ICMP Code: 0
<p>Impact</p> <p>This information could theoretically be used to exploit weak time-based random number generators in other services.</p>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>Various mitigations are possible:</p> <ul style="list-style-type: none"> - 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: 2023-05-11T09:09:33Z

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

dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.130 \]](#)

2.33 192.168.0.61

Host scan start Sun May 5 03:01:09 2024 UTC

Host scan end Sun May 5 04:28:33 2024 UTC

Service (Port)	Threat Level
443/tcp	Medium
general/icmp	Low
22/tcp	Low

2.33.1 Medium 443/tcp

Medium (CVSS: 4.3)

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

Summary

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

Quality of Detection: 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>Impact</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>Solution:</p> <p>Solution type: 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>Affected Software/OS</p> <p>All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.</p>
<p>Vulnerability Insight</p> <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: 2023-10-20T16:09:12Z</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 ↪-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>
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/1751
 cert-bund: CB-K15/1266
 cert-bund: CB-K15/0850
 cert-bund: CB-K15/0764
 cert-bund: CB-K15/0720
 cert-bund: CB-K15/0548
 cert-bund: CB-K15/0526
 cert-bund: CB-K15/0509
 cert-bund: CB-K15/0493
 cert-bund: CB-K15/0384
 cert-bund: CB-K15/0365
 cert-bund: CB-K15/0364
 cert-bund: CB-K15/0302
 cert-bund: CB-K15/0192
 cert-bund: CB-K15/0079
 cert-bund: CB-K15/0016
 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

...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482

[\[return to 192.168.0.61 \]](#)

2.33.2 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: 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: 2023-05-11T09:09:33Z
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
... continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.61 \]](#)**2.33.3 Low 22/tcp**

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary

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

Quality of Detection: 80**Vulnerability Detection Result**The remote SSH server supports the following weak client-to-server MAC algorithm \hookrightarrow (s):

umac-64-etm@openssh.com

umac-64@openssh.com

The remote SSH server supports the following weak server-to-client MAC algorithm \hookrightarrow (s):

umac-64-etm@openssh.com

umac-64@openssh.com

Solution:**Solution type:** Mitigation

Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method

Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.

Currently weak MAC algorithms are defined as the following:

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

Details: Weak MAC Algorithm(s) Supported (SSH)

OID:1.3.6.1.4.1.25623.1.0.105610

Version used: 2023-10-12T05:05:32Z

Referencesurl: <https://www.rfc-editor.org/rfc/rfc6668>url: <https://www.rfc-editor.org/rfc/rfc4253#section-6.4>

[\[return to 192.168.0.61 \]](#)

2.34 192.168.0.97

Host scan start Sun May 5 04:10:01 2024 UTC
Host scan end Sun May 5 05:26:20 2024 UTC

Service (Port)	Threat Level
443/tcp	Medium

2.34.1 Medium 443/tcp

Medium (CVSS: 4.3)

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

Summary

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

Quality of Detection: 98

Vulnerability Detection Result

In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.1 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.80.2067) 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: 2023-10-20T16:09:12Z</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: 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-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> <p>dfn-cert: DFN-CERT-2019-0068</p>
...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418

...continues on next page ...

...continued from previous page ...	
dfn-cert:	DFN-CERT-2012-0354
dfn-cert:	DFN-CERT-2012-0234
dfn-cert:	DFN-CERT-2012-0221
dfn-cert:	DFN-CERT-2012-0177
dfn-cert:	DFN-CERT-2012-0170
dfn-cert:	DFN-CERT-2012-0146
dfn-cert:	DFN-CERT-2012-0142
dfn-cert:	DFN-CERT-2012-0126
dfn-cert:	DFN-CERT-2012-0123
dfn-cert:	DFN-CERT-2012-0095
dfn-cert:	DFN-CERT-2012-0051
dfn-cert:	DFN-CERT-2012-0047
dfn-cert:	DFN-CERT-2012-0021
dfn-cert:	DFN-CERT-2011-1953
dfn-cert:	DFN-CERT-2011-1946
dfn-cert:	DFN-CERT-2011-1844
dfn-cert:	DFN-CERT-2011-1826
dfn-cert:	DFN-CERT-2011-1774
dfn-cert:	DFN-CERT-2011-1743
dfn-cert:	DFN-CERT-2011-1738
dfn-cert:	DFN-CERT-2011-1706
dfn-cert:	DFN-CERT-2011-1628
dfn-cert:	DFN-CERT-2011-1627
dfn-cert:	DFN-CERT-2011-1619
dfn-cert:	DFN-CERT-2011-1482

[\[return to 192.168.0.97 \]](#)

2.35 192.168.0.245

Host scan start Sun May 5 03:42:08 2024 UTC
Host scan end Sun May 5 04:18:51 2024 UTC

Service (Port)	Threat Level
general/icmp	Low
22/tcp	Low

2.35.1 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
Summary
... continues on next page ...

...continued from previous page ...
The remote host responded to an ICMP timestamp request.
Quality of Detection: 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.245 \]](#)

2.35.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)
Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).
Quality of Detection: 80
Vulnerability Detection Result The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s): umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm ↪(s): umac-64-etm@openssh.com umac-64@openssh.com
Solution: Solution type: Mitigation Disable the reported weak MAC algorithm(s).
Vulnerability Detection Method Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[\[return to 192.168.0.245 \]](#)

2.36 192.168.0.67

Host scan start Sun May 5 03:42:56 2024 UTC
Host scan end Sun May 5 04:17:12 2024 UTC

Service (Port)	Threat Level
22/tcp	Low
general/icmp	Low

2.36.1 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)
Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).
Quality of Detection: 80
Vulnerability Detection Result The remote SSH server supports the following weak client-to-server MAC algorithm $\hookrightarrow(s)$: umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm $\hookrightarrow(s)$: umac-64-etm@openssh.com umac-64@openssh.com
Solution: Solution type: Mitigation Disable the reported weak MAC algorithm(s).
Vulnerability Detection Method Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[[return to 192.168.0.67](#)]

2.36.2 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: 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.67 \]](#)

2.37 192.168.0.131

Host scan start Sun May 5 03:01:04 2024 UTC
Host scan end Sun May 5 03:32:43 2024 UTC

Service (Port)	Threat Level
general/icmp	Low
22/tcp	Low

2.37.1 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: 80
Vulnerability Detection Result The following response / ICMP packet has been received: <ul style="list-style-type: none">- 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: <ul style="list-style-type: none">- 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
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.131 \]](#)

2.37.2 Low 22/tcp

Low (CVSS: 2.6) NVT: Weak MAC Algorithm(s) Supported (SSH)
Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).
Quality of Detection: 80
Vulnerability Detection Result The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s): umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm ↪(s): umac-64-etm@openssh.com umac-64@openssh.com
Solution: Solution type: Mitigation Disable the reported weak MAC algorithm(s).
Vulnerability Detection Method Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: <ul style="list-style-type: none"> - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms
... continues on next page ...

...continued from previous page ...
- 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[\[return to 192.168.0.131 \]](#)

2.38 192.168.0.217

Host scan start Sun May 5 03:01:04 2024 UTC
Host scan end Sun May 5 03:30:44 2024 UTC

Service (Port)	Threat Level
general/icmp	Low
22/tcp	Low

2.38.1 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: 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)
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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[[return to 192.168.0.217](#)]

2.38.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)
Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).
Quality of Detection: 80
Vulnerability Detection Result The remote SSH server supports the following weak client-to-server MAC algorithm $\hookrightarrow(s)$: umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm $\hookrightarrow(s)$: umac-64-etm@openssh.com umac-64@openssh.com
... continues on next page ...

...continued from previous page ...
Solution: Solution type: Mitigation Disable the reported weak MAC algorithm(s).
Vulnerability Detection Method Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[[return to 192.168.0.217](#)]

2.39 192.168.0.234

Host scan start Sun May 5 03:40:51 2024 UTC
Host scan end Sun May 5 05:04:50 2024 UTC

Service (Port)	Threat Level
22/tcp	Low
general/icmp	Low

2.39.1 Low 22/tcp

Low (CVSS: 2.6) NVT: Weak MAC Algorithm(s) Supported (SSH)
Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).
Quality of Detection: 80
... continues on next page ...

...continued from previous page ...

Vulnerability Detection Result

The remote SSH server supports the following weak client-to-server MAC algorithm $\hookrightarrow(s)$:

umac-64-etm@openssh.com

umac-64@openssh.com

The remote SSH server supports the following weak server-to-client MAC algorithm $\hookleftarrow(s)$:

umac-64-etm@openssh.com

umac-64@openssh.com

Solution:

Solution type: Mitigation

Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method

Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.

Currently weak MAC algorithms are defined as the following:

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

Details: Weak MAC Algorithm(s) Supported (SSH)

OID:1.3.6.1.4.1.25623.1.0.105610

Version used: 2023-10-12T05:05:32Z

References

url: <https://www.rfc-editor.org/rfc/rfc6668>

url: <https://www.rfc-editor.org/rfc/rfc4253#section-6.4>

[\[return to 192.168.0.234 \]](#)

2.39.2 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: 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: 2023-05-11T09:09:33Z

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

dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.234 \]](#)

2.40 192.168.0.233

Host scan start Sun May 5 03:38:58 2024 UTC

Host scan end Sun May 5 05:04:38 2024 UTC

Service (Port)	Threat Level
general/icmp	Low
22/tcp	Low

2.40.1 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: 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.233 \]](#)

2.40.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)
Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).
Quality of Detection: 80
Vulnerability Detection Result The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s): umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm ↪(s): umac-64-etm@openssh.com umac-64@openssh.com
Solution: Solution type: Mitigation Disable the reported weak MAC algorithm(s).
Vulnerability Detection Method Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[[return to 192.168.0.233](#)]

2.41 192.168.0.232

Host scan start Sun May 5 03:32:44 2024 UTC

Host scan end Sun May 5 04:58:08 2024 UTC

Service (Port)	Threat Level
general/icmp	Low
22/tcp	Low

2.41.1 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: 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

... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.232 \]](#)

2.41.2 Low 22/tcp

Low (CVSS: 2.6) NVT: Weak MAC Algorithm(s) Supported (SSH)
Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).
Quality of Detection: 80
Vulnerability Detection Result The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s): umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm ↪(s): umac-64-etm@openssh.com umac-64@openssh.com
Solution: Solution type: Mitigation Disable the reported weak MAC algorithm(s).
Vulnerability Detection Method Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms
... continues on next page ...

...continued from previous page ...

- 'none' algorithm
 Details: Weak MAC Algorithm(s) Supported (SSH)
 OID:1.3.6.1.4.1.25623.1.0.105610
 Version used: 2023-10-12T05:05:32Z

References

url: <https://www.rfc-editor.org/rfc/rfc6668>

url: <https://www.rfc-editor.org/rfc/rfc4253#section-6.4>

[[return to 192.168.0.232](#)]

2.42 192.168.0.126

Host scan start Sun May 5 03:37:59 2024 UTC

Host scan end Sun May 5 04:50:38 2024 UTC

Service (Port)	Threat Level
general/icmp	Low
22/tcp	Low

2.42.1 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: 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)
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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[[return to 192.168.0.126](#)]

2.42.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)
Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).
Quality of Detection: 80
Vulnerability Detection Result The remote SSH server supports the following weak client-to-server MAC algorithm \hookrightarrow (s): umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm \hookrightarrow (s): umac-64-etm@openssh.com umac-64@openssh.com
... continues on next page ...

...continued from previous page ...
Solution: Solution type: Mitigation Disable the reported weak MAC algorithm(s).
Vulnerability Detection Method Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[[return to 192.168.0.126](#)]

2.43 192.168.0.248

Host scan start Sun May 5 03:30:45 2024 UTC
Host scan end Sun May 5 04:51:03 2024 UTC

Service (Port)	Threat Level
22/tcp	Low
general/icmp	Low

2.43.1 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)
Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).
Quality of Detection: 80
... continues on next page ...

...continued from previous page ...

Vulnerability Detection Result

The remote SSH server supports the following weak client-to-server MAC algorithm $\hookrightarrow(s)$:

umac-64-etm@openssh.com

umac-64@openssh.com

The remote SSH server supports the following weak server-to-client MAC algorithm $\hookleftarrow(s)$:

umac-64-etm@openssh.com

umac-64@openssh.com

Solution:

Solution type: Mitigation

Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method

Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.

Currently weak MAC algorithms are defined as the following:

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

Details: Weak MAC Algorithm(s) Supported (SSH)

OID:1.3.6.1.4.1.25623.1.0.105610

Version used: 2023-10-12T05:05:32Z

References

url: <https://www.rfc-editor.org/rfc/rfc6668>

url: <https://www.rfc-editor.org/rfc/rfc4253#section-6.4>

[\[return to 192.168.0.248 \]](#)

2.43.2 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: 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: 2023-05-11T09:09:33Z

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

dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.248 \]](#)

2.44 192.168.0.208

Host scan start Sun May 5 04:10:04 2024 UTC

Host scan end Sun May 5 05:08:50 2024 UTC

Service (Port)	Threat Level
general/icmp	Low
22/tcp	Low

2.44.1 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: 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.208 \]](#)

2.44.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)
Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).
Quality of Detection: 80
Vulnerability Detection Result The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s): umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm ↪(s): umac-64-etm@openssh.com umac-64@openssh.com
Solution: Solution type: Mitigation Disable the reported weak MAC algorithm(s).
Vulnerability Detection Method Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[[return to 192.168.0.208](#)]

2.45 192.168.0.211

Host scan start Sun May 5 03:01:04 2024 UTC

Host scan end Sun May 5 03:45:13 2024 UTC

Service (Port)	Threat Level
general/icmp	Low
22/tcp	Low

2.45.1 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: 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

... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.211 \]](#)

2.45.2 Low 22/tcp

Low (CVSS: 2.6) NVT: Weak MAC Algorithm(s) Supported (SSH)
Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).
Quality of Detection: 80
Vulnerability Detection Result The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s): umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm ↪(s): umac-64-etm@openssh.com umac-64@openssh.com
Solution: Solution type: Mitigation Disable the reported weak MAC algorithm(s).
Vulnerability Detection Method Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: <ul style="list-style-type: none"> - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms
... continues on next page ...

...continued from previous page ...
- 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[\[return to 192.168.0.211 \]](#)

2.46 192.168.0.160

Host scan start Sun May 5 03:01:04 2024 UTC
Host scan end Sun May 5 03:29:04 2024 UTC

Service (Port)	Threat Level
general/icmp	Low

2.46.1 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: 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)
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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[[return to 192.168.0.160](#)]

2.47 192.168.0.35

Host scan start Sun May 5 03:01:04 2024 UTC
Host scan end Sun May 5 03:31:32 2024 UTC

Service (Port)	Threat Level
general/icmp	Low

2.47.1 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: 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: 2023-05-11T09:09:33Z

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

dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.35 \]](#)

2.48 192.168.0.161

Host scan start Sun May 5 03:01:04 2024 UTC

Host scan end Sun May 5 03:48:29 2024 UTC

Service (Port)	Threat Level
general/icmp	Low

2.48.1 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: 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: 2023-05-11T09:09:33Z
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 dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.0.161 \]](#)

This file was automatically generated.