

Scan Report

November 24, 2025

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Immediate scan of IP 192.168.220.129”. The scan started at Mon Nov 24 15:05:38 2025 UTC and ended at Mon Nov 24 15:42:42 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1	Result Overview	2
1.1	Host Authentications	2
2	Results per Host	2
2.1	192.168.220.129	2
2.1.1	High 513/tcp	3
2.1.2	High 6697/tcp	4
2.1.3	High 80/tcp	6
2.1.4	High 5432/tcp	8
2.1.5	High 21/tcp	10
2.1.6	High 1099/tcp	12
2.1.7	High 514/tcp	13
2.1.8	High 2121/tcp	14
2.1.9	Medium 22/tcp	16
2.1.10	Medium 80/tcp	20
2.1.11	Medium 25/tcp	34
2.1.12	Medium 5432/tcp	53
2.1.13	Medium 21/tcp	70
2.1.14	Medium 5900/tcp	72
2.1.15	Medium 23/tcp	73
2.1.16	Medium 2121/tcp	74
2.1.17	Medium 445/tcp	74

CONTENTS	2
----------	---

2.1.18 Low 22/tcp	76
2.1.19 Low 25/tcp	77
2.1.20 Low general/tcp	83
2.1.21 Low general/icmp	84
2.1.22 Low 5432/tcp	86

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.220.129	10	40	6	0	0
Total: 1	10	40	6	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 56 results selected by the filtering described above. Before filtering there were 633 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.220.129	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 192.168.220.129

Host scan start Mon Nov 24 15:06:14 2025 UTC

Host scan end Mon Nov 24 15:42:13 2025 UTC

Service (Port)	Threat Level
513/tcp	High
6697/tcp	High
80/tcp	High
5432/tcp	High
21/tcp	High
1099/tcp	High
514/tcp	High
2121/tcp	High
22/tcp	Medium

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
80/tcp	Medium
25/tcp	Medium
5432/tcp	Medium
21/tcp	Medium
5900/tcp	Medium
23/tcp	Medium
2121/tcp	Medium
445/tcp	Medium
22/tcp	Low
25/tcp	Low
general/tcp	Low
general/icmp	Low
5432/tcp	Low

2.1.1 High 513/tcp

High (CVSS: 7.5)
NVT: The rlogin service is running
<p>Summary This remote host is running a rlogin service.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result The rlogin service is running on the target system.</p>
<p>Solution: Solution type: Mitigation Disable the rlogin service and use alternatives like SSH instead.</p>
<p>Vulnerability Insight rlogin has several serious security problems, - all information, including passwords, is transmitted unencrypted. - .rlogin (or .rhosts) file is easy to misuse (potentially allowing anyone to login without a password)</p>
<p>Vulnerability Detection Method Details: The rlogin service is running OID:1.3.6.1.4.1.25623.1.0.901202 Version used: 2025-03-05T05:38:53Z</p>
<p>References ... continues on next page ...</p>

	... continued from previous page ...
cve:	CVE-1999-0651

[[return to 192.168.220.129](#)]

2.1.2 High 6697/tcp

High (CVSS: 8.1)
NVT: UnrealIRCd Authentication Spoofing Vulnerability
Product detection result cpe:/a:unrealircd:unrealircd:3.2.8.1 Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)
Summary UnrealIRCd is prone to authentication spoofing vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 3.2.8.1 Fixed version: 3.2.10.7
Impact Successful exploitation of this vulnerability will allow remote attackers to spoof certificate fingerprints and consequently log in as another user.
Solution: Solution type: VendorFix Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.
Affected Software/OS UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.
Vulnerability Insight The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: UnrealIRCd Authentication Spoofing Vulnerability OID:1.3.6.1.4.1.25623.1.0.809883 Version used: 2023-07-14T16:09:27Z
... continues on next page ...

... continued from previous page ...

Product Detection Result

Product: cpe:/a:unrealircd:unrealircd:3.2.8.1
Method: UnrealIRCd Detection
OID: 1.3.6.1.4.1.25623.1.0.809884)

References

cve: CVE-2016-7144
url: <http://seclists.org/oss-sec/2016/q3/420>
url: <http://www.securityfocus.com/bid/92763>
url: <http://www.openwall.com/lists/oss-security/2016/09/05/8>
url: <https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86b>
↪c50ba1a34a766
url: https://bugs.unrealircd.org/main_page.php

High (CVSS: 7.5)

NVT: UnrealIRCd Backdoor

Product detection result

cpe:/a:unrealircd:unrealircd:3.2.8.1
Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)

Summary

Detection of backdoor in UnrealIRCd.

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

Vulnerability was detected according to the Vulnerability Detection Method.

Solution:

Solution type: VendorFix

Install latest version of unrealircd and check signatures of software you're installing.

Affected Software/OS

The issue affects Unreal 3.2.8.1 for Linux. Reportedly package Unreal3.2.8.1.tar.gz downloaded in November 2009 and later is affected. The MD5 sum of the affected file is 752e46f2d873c1679fa99de3f52a274d. Files with MD5 sum of 7b741e94e867c0a7370553fd01506c66 are not affected.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...
Remote attackers can exploit this issue to execute arbitrary system commands within the context of the affected application.
Vulnerability Detection Method Details: UnrealIRCd Backdoor OID:1.3.6.1.4.1.25623.1.0.80111 Version used: 2025-03-21T05:38:29Z
Product Detection Result Product: cpe:/a:unrealircd:unrealircd:3.2.8.1 Method: UnrealIRCd Detection OID: 1.3.6.1.4.1.25623.1.0.809884)
References cve: CVE-2010-2075 url: http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt url: http://seclists.org/fulldisclosure/2010/Jun/277 url: http://www.securityfocus.com/bid/40820

[[return to 192.168.220.129](#)]

2.1.3 High 80/tcp

High (CVSS: 7.5)
NVT: Test HTTP dangerous methods
Summary Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE.
Quality of Detection (QoD): 99%
Vulnerability Detection Result We could upload the following files via the PUT method at this web server: http://192.168.220.129/dav/puttest615857866.html We could delete the following files via the DELETE method at this web server: http://192.168.220.129/dav/puttest615857866.html
Impact - Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server. - Enabled DELETE method: This might allow an attacker to delete additional files on this web server.
... continues on next page ...

<p style="text-align: right;">... continued from previous page ...</p> <p>Solution: Solution type: Mitigation Use access restrictions to these dangerous HTTP methods or disable them completely.</p> <p>Affected Software/OS Web servers with enabled PUT and/or DELETE methods.</p> <p>Vulnerability Detection Method Checks if dangerous HTTP methods such as PUT and DELETE are enabled and can be misused to upload or delete files. Details: Test HTTP dangerous methods OID:1.3.6.1.4.1.25623.1.0.10498 Version used: 2023-08-01T13:29:10Z</p> <p>References url: http://www.securityfocus.com/bid/12141 owasp: OWASP-CM-001</p>
--

<p>High (CVSS: 7.5)</p> <p>NVT: EasyPHP Webserver <= 12.1 Multiple Vulnerabilities - Active Check</p> <p>Summary EasyPHP Webserver is prone to multiple vulnerabilities.</p> <p>Quality of Detection (QoD): 99%</p> <p>Vulnerability Detection Result Vulnerable URL: http://192.168.220.129/phpinfo.php Concluded from: <pre><title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX, NOFOLLOW, NOARCHIV ↪E" /></head> <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph ↪p5/cgi </td></tr> <h2>PHP Core</h2> <h2>PHP Variables</h2></pre> </p> <p>Impact Successful exploitation will allow attackers to gain administrative access, disclose the information, inject PHP code/shell and execute a remote PHP Code.</p> <p>Solution: Solution type: WillNotFix</p>
--

... continues on next page ...

<p>... continued from previous page ...</p> <p>No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.</p>
<p>Affected Software/OS EasyPHP version 12.1 and prior.</p>
<p>Vulnerability Insight The bug in EasyPHP WebServer Manager, its skipping authentication for certain requests. Which allows to bypass the authentication, disclose the information or execute a remote PHP code.</p>
<p>Vulnerability Detection Method Sends a crafted HTTP GET request and checks the response. Note: It is currently expected that a result of this VT is reported if the system is generally exposing a phpinfo() output on the relevant URL / endpoint (independent from the running product). Exposing such sensitive information is generally seen as a security misconfiguration and should be avoided. Details: EasyPHP Webserver <= 12.1 Multiple Vulnerabilities - Active Check OID:1.3.6.1.4.1.25623.1.0.803189 Version used: 2025-11-11T05:40:18Z</p>
<p>References url: https://cxsecurity.com/issue/WLB-2013040069</p>

[[return to 192.168.220.129](#)]

2.1.4 High 5432/tcp

<p>High (CVSS: 7.4)</p> <p>NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability</p>
<p>Summary OpenSSL is prone to a security bypass vulnerability.</p>
<p>Quality of Detection (QoD): 70%</p>
<p>Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p>Impact Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.</p>
<p>... continues on next page ...</p>

... continued from previous page ...

Solution:**Solution type:** VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h.

Vulnerability Insight

OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

Vulnerability Detection Method

Send two SSL ChangeCipherSpec request and check the response.

Details: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

OID:1.3.6.1.4.1.25623.1.0.105042

Version used: 2025-01-17T15:39:18Z

References

cve: CVE-2014-0224

url: <https://www.openssl.org/news/secadv/20140605.txt>

url: <http://www.securityfocus.com/bid/67899>

cert-bund: WID-SEC-2023-0500

cert-bund: CB-K15/0567

cert-bund: CB-K15/0415

cert-bund: CB-K15/0384

cert-bund: CB-K15/0080

cert-bund: CB-K15/0079

cert-bund: CB-K15/0074

cert-bund: CB-K14/1617

cert-bund: CB-K14/1537

cert-bund: CB-K14/1299

cert-bund: CB-K14/1297

cert-bund: CB-K14/1294

cert-bund: CB-K14/1202

cert-bund: CB-K14/1174

cert-bund: CB-K14/1153

cert-bund: CB-K14/0876

cert-bund: CB-K14/0756

cert-bund: CB-K14/0746

cert-bund: CB-K14/0736

cert-bund: CB-K14/0722

cert-bund: CB-K14/0716

cert-bund: CB-K14/0708

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K14/0684
cert-bund: CB-K14/0683
cert-bund: CB-K14/0680
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-0593
dfn-cert: DFN-CERT-2015-0427
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0078
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1364
dfn-cert: DFN-CERT-2014-1357
dfn-cert: DFN-CERT-2014-1350
dfn-cert: DFN-CERT-2014-1265
dfn-cert: DFN-CERT-2014-1209
dfn-cert: DFN-CERT-2014-0917
dfn-cert: DFN-CERT-2014-0789
dfn-cert: DFN-CERT-2014-0778
dfn-cert: DFN-CERT-2014-0768
dfn-cert: DFN-CERT-2014-0752
dfn-cert: DFN-CERT-2014-0747
dfn-cert: DFN-CERT-2014-0738
dfn-cert: DFN-CERT-2014-0715
dfn-cert: DFN-CERT-2014-0714
dfn-cert: DFN-CERT-2014-0709
```

[[return to 192.168.220.129](#)]

2.1.5 High 21/tcp

High (CVSS: 7.5)

NVT: FTP Brute Force Logins With Default Credentials Reporting

Summary

It was possible to login into the remote FTP server using weak/known credentials.

Quality of Detection (QoD): 95%

Vulnerability Detection Result

It was possible to login with the following credentials <User>:<Password>

msfadmin:msfadmin

postgres:postgres

... continues on next page ...

	... continued from previous page ...
service:service user:user	
Impact This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.	
Solution: Solution type: Mitigation Change the password as soon as possible.	
Vulnerability Insight The following devices are / software is known to be affected: <ul style="list-style-type: none"> - CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R - CVE-2013-7404: GE Healthcare Discovery NM 750b - CVE-2014-9198: Schneider Electric ETG3000 FactoryCast HMI gateways - CVE-2015-7261: QNAP iArtist Lite distributed with QNAP Signage Station - CVE-2016-8731: Foscam C1 devices - CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices - CVE-2018-9068: IMM2 for IBM and Lenovo System x - CVE-2018-17771: Ingenico Telium 2 PoS terminals - CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices <p>Note: As the VT 'FTP Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.</p>	
Vulnerability Detection Method Reports weak/known credentials detected by the VT 'FTP Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108717). Details: FTP Brute Force Logins With Default Credentials Reporting OID:1.3.6.1.4.1.25623.1.0.108718 Version used: 2025-05-13T05:41:39Z	
References cve: CVE-1999-0501 cve: CVE-1999-0502 cve: CVE-1999-0507 cve: CVE-1999-0508 cve: CVE-2001-1594 cve: CVE-2013-7404 cve: CVE-2014-9198 cve: CVE-2015-7261 cve: CVE-2016-8731 cve: CVE-2017-8218 cve: CVE-2018-9068 cve: CVE-2018-17771	
... continues on next page ...	

... continued from previous page ...
cve: CVE-2018-19063
cve: CVE-2018-19064

[[return to 192.168.220.129](#)]

2.1.6 High 1099/tcp

High (CVSS: 7.5)

NVT: Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check

Summary

Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code (remote code execution/RCE) on a targeted system with elevated privileges.

Quality of Detection (QoD): 95%

Vulnerability Detection Result

By doing an RMI request it was possible to trigger the vulnerability and make the remote host sending a request back to the scanner host (Details on the received packet follows).

Destination IP: 192.168.220.128 (receiving IP on scanner host side)

Destination port: 21657/tcp (receiving port on scanner host side)

Originating IP: 192.168.220.129 (originating IP from target host side)

Impact

An unauthenticated, remote attacker could exploit the vulnerability by transmitting crafted packets to the affected software. When the packets are processed, the attacker could execute arbitrary code on the system with elevated privileges.

Solution:

Solution type: Workaround

Disable class-loading. Please contact the vendor of the affected system for additional guidance.

Vulnerability Insight

The vulnerability exists because of an incorrect default configuration of the Remote Method Invocation (RMI) Server in the affected software.

Vulnerability Detection Method

Sends a crafted JRMI request and checks if the target is connecting back to the scanner host.

Note: For a successful detection of this flaw the target host needs to be able to reach the scanner host on a TCP port randomly generated during the runtime of the VT (currently in the range of 10000-32000).

... continues on next page ...

... continued from previous page ...	
Details: Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check	Check
OID:1.3.6.1.4.1.25623.1.0.140051	
Version used: 2025-04-11T15:45:04Z	
References	
cve: CVE-2011-3556	
url: https://web.archive.org/web/20211208040855/http://www.securitytracker.com/id?1026215	
url: https://web.archive.org/web/20110824060234/http://download.oracle.com/java/e/1.3/docs/guide/rmi/spec/rmi-protocol.html	
url: https://tools.cisco.com/security/center/viewAlert.x?alertId=23665	
dfn-cert: DFN-CERT-2012-1829	
dfn-cert: DFN-CERT-2012-1380	
dfn-cert: DFN-CERT-2012-1377	
dfn-cert: DFN-CERT-2012-1156	
dfn-cert: DFN-CERT-2012-1155	
dfn-cert: DFN-CERT-2012-0956	
dfn-cert: DFN-CERT-2012-0828	
dfn-cert: DFN-CERT-2012-0815	
dfn-cert: DFN-CERT-2012-0638	
dfn-cert: DFN-CERT-2012-0451	
dfn-cert: DFN-CERT-2012-0418	
dfn-cert: DFN-CERT-2012-0354	
dfn-cert: DFN-CERT-2012-0146	
dfn-cert: DFN-CERT-2012-0142	
dfn-cert: DFN-CERT-2012-0126	
dfn-cert: DFN-CERT-2012-0095	
dfn-cert: DFN-CERT-2012-0047	
dfn-cert: DFN-CERT-2011-1844	
dfn-cert: DFN-CERT-2011-1826	
dfn-cert: DFN-CERT-2011-1804	
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	

[[return to 192.168.220.129](#)]

2.1.7 High 514/tcp

High (CVSS: 7.5)
NVT: rsh Unencrypted Cleartext Login
Summary This remote host is running a rsh service.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The rsh service is misconfigured so it is allowing connections without a password or with default root:root credentials.
Solution: Solution type: Mitigation Disable the rsh service and use alternatives like SSH instead.
Vulnerability Insight rsh (remote shell) is a command line computer program which can execute shell commands as another user, and on another computer across a computer network. 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: rsh Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.100080 Version used: 2021-10-20T09:03:29Z
References cve: CVE-1999-0651

[[return to 192.168.220.129](#)]

2.1.8 High 2121/tcp

High (CVSS: 7.5)
NVT: FTP Brute Force Logins With Default Credentials Reporting
Summary It was possible to login into the remote FTP server using weak/known credentials.
Quality of Detection (QoD): 95%
... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

It was possible to login with the following credentials <User>:<Password>
msfadmin:msfadmin
postgres:postgres
service:service
user:user

Impact

This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

Solution:

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Insight

The following devices / software is known to be affected:

- CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R
- CVE-2013-7404: GE Healthcare Discovery NM 750b
- CVE-2014-9198: Schneider Electric ETG3000 FactoryCast HMI gateways
- CVE-2015-7261: QNAP iArtist Lite distributed with QNAP Signage Station
- CVE-2016-8731: Foscam C1 devices
- CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices
- CVE-2018-9068: IMM2 for IBM and Lenovo System x
- CVE-2018-17771: Ingenico Telium 2 PoS terminals
- CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices

Note: As the VT 'FTP Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method

Reports weak/known credentials detected by the VT 'FTP Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108717).

Details: **FTP Brute Force Logins With Default Credentials Reporting**

OID:1.3.6.1.4.1.25623.1.0.108718

Version used: 2025-05-13T05:41:39Z

References

cve: CVE-1999-0501
cve: CVE-1999-0502
cve: CVE-1999-0507
cve: CVE-1999-0508
cve: CVE-2001-1594
cve: CVE-2013-7404
cve: CVE-2014-9198

... continues on next page ...

<pre>cve: CVE-2015-7261 cve: CVE-2016-8731 cve: CVE-2017-8218 cve: CVE-2018-9068 cve: CVE-2018-17771 cve: CVE-2018-19063 cve: CVE-2018-19064</pre>	... continued from previous page ...
--	--------------------------------------

[\[return to 192.168.220.129 \]](#)

2.1.9 Medium 22/tcp

Medium (CVSS: 5.3)

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

Product detection result

cpe:/a:ietf:secure_shell_protocol

Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 →)
--

Summary

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

Quality of Detection (QoD): 80%
--

Vulnerability Detection Result

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

KEX algorithm Reason

----- →-----

diffie-hellman-group-exchange-sha1 Using SHA-1 diffie-hellman-group1-sha1 Using Oakley Group 2 (a 1024-bit MODP group →) and SHA-1
--

Impact

An attacker can quickly break individual connections.

Solution:

Solution type: Mitigation

Disable the reported weak KEX algorithm(s)
--

- 1024-bit MODP group / prime KEX algorithms:

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

... continues on next page ...

... continued from previous page ...

Vulnerability Insight

- 1024-bit MODP group / prime KEX algorithms:

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

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

Vulnerability Detection Method

Checks the supported KEX algorithms of the remote SSH server.

Currently weak KEX algorithms are defined as the following:

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

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

OID: 1.3.6.1.4.1.25623.1.0.150713

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

Product Detection Result

Product: cpe:/a:ietf:secure_shell_protocol

Method: SSH Protocol Algorithms Supported

OID: 1.3.6.1.4.1.25623.1.0.105565)

References

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

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

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

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

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

Medium (CVSS: 5.3)

NVT: Weak Host Key Algorithm(s) (SSH)

Product detection result

cpe:/a:ietf:secure_shell_protocol

Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565

↔)

Summary

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

... continues on next page ...

	... continued from previous page ...				
Quality of Detection (QoD): 80%					
<p>Vulnerability Detection Result</p> <p>The remote SSH server supports the following weak host key algorithm(s):</p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding-bottom: 5px;">host key algorithm</th> <th style="text-align: left; padding-bottom: 5px;"> Description</th> </tr> </thead> <tbody> <tr> <td style="padding-top: 5px;">ssh-dss</td> <td style="padding-top: 5px;"> Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)</td> </tr> </tbody> </table>		host key algorithm	Description	ssh-dss	Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
host key algorithm	Description				
ssh-dss	Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)				
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>Disable the reported weak host key algorithm(s).</p>					
<p>Vulnerability Detection Method</p> <p>Checks the supported host key algorithms of the remote SSH server.</p> <p>Currently weak host key algorithms are defined as the following:</p> <ul style="list-style-type: none"> - ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS) <p>Details: Weak Host Key Algorithm(s) (SSH) OID:1.3.6.1.4.1.25623.1.0.117687 Version used: 2024-06-14T05:05:48Z</p>					
<p>Product Detection Result</p> <p>Product: cpe:/a:ietf:secure_shell_protocol</p> <p>Method: SSH Protocol Algorithms Supported OID: 1.3.6.1.4.1.25623.1.0.105565)</p>					
<p>References</p> <p>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</p>					

	Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)	
<p>Product detection result</p> <p>cpe:/a:ietf:secure_shell_protocol</p> <p>Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↔)</p>	
<p>Summary</p>	
... continues on next page ...	

<p>... continued from previous page ...</p> <p>The remote SSH server is configured to allow / support weak encryption algorithm(s).</p> <p>Quality of Detection (QoD): 80%</p> <p>Vulnerability Detection Result</p> <p>The remote SSH server supports the following weak client-to-server encryption algorithms:</p> <pre>3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se</pre> <p>The remote SSH server supports the following weak server-to-client encryption algorithms:</p> <pre>3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se</pre>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>Disable the reported weak encryption algorithm(s).</p>
<p>Vulnerability Insight</p> <ul style="list-style-type: none"> - 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.
<p>Vulnerability Detection Method</p> <p>Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.</p>

... continues on next page ...

<p>... continued from previous page ...</p> <p>Currently weak encryption algorithms are defined as the following:</p> <ul style="list-style-type: none"> - Arcfour (RC4) cipher based algorithms - 'none' algorithm - CBC mode cipher based algorithms <p>Details: Weak Encryption Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105611 Version used: 2024-06-14T05:05:48Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:ietf:secure_shell_protocol Method: SSH Protocol Algorithms Supported OID: 1.3.6.1.4.1.25623.1.0.105565)</p>
<p>References</p> <p>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</p>

[[return to 192.168.220.129](#)]

2.1.10 Medium 80/tcp

<p>Medium (CVSS: 6.8)</p> <p>NVT: TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)</p>
<p>Summary</p> <p>TWiki is prone to a cross-site request forgery (CSRF) vulnerability.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 01.Feb.2003 Fixed version: 4.3.2</p>
<p>Impact</p> <p>Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.</p>
<p>Solution:</p> <p>Solution type: VendorFix Upgrade to TWiki version 4.3.2 or later.</p>
<p>... continues on next page ...</p>

	... continued from previous page ...
Affected Software/OS	TWiki version prior to 4.3.2
Vulnerability Insight	Attack can be done by tricking an authenticated TWiki user into visiting a static HTML page on another side, where a Javascript enabled browser will send an HTTP POST request to TWiki, which in turn will process the request as the TWiki user.
Vulnerability Detection Method	Details: TWiki Cross-Site Request Forgery Vulnerability (Sep 2010) OID:1.3.6.1.4.1.25623.1.0.801281 Version used: 2024-03-01T14:37:10Z
References	<p>cve: CVE-2009-4898</p> <p>url: http://www.openwall.com/lists/oss-security/2010/08/03/8</p> <p>url: http://www.openwall.com/lists/oss-security/2010/08/02/17</p> <p>url: http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix</p> <p>url: http://twiki.org/cgi-bin/view/Codev/DownloadTWiki</p>

Medium (CVSS: 6.1)
NVT: TWiki < 6.1.0 XSS Vulnerability
Summary bin/statistics in TWiki 6.0.2 allows XSS via the webs parameter.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 01.Feb.2003 Fixed version: 6.1.0
Solution: Solution type: VendorFix Update to version 6.1.0 or later.
Affected Software/OS TWiki version 6.0.2 and probably prior.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: TWiki < 6.1.0 XSS Vulnerability OID:1.3.6.1.4.1.25623.1.0.141830

... continues on next page ...

	... continued from previous page ...
	Version used: 2023-07-14T16:09:27Z

References

cve: CVE-2018-20212
 url: <https://seclists.org/fulldisclosure/2019/Jan/7>
 url: <http://twiki.org/cgi-bin/view/Codev/DownloadTWiki>

Medium (CVSS: 6.1)

NVT: jQuery < 1.9.0 XSS Vulnerability

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

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

Installed version: 1.3.2

Fixed version: 1.9.0

Installation

path / port: /mutillidae/javascript/ddsmoothmenu/jquery.min.js

Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):

- Identified file: <http://192.168.220.129/mutillidae/javascript/ddsmoothmenu/jquery.min.js>
- Referenced at: <http://192.168.220.129/mutillidae/>

Solution:

Solution type: VendorFix

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Insight

The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method

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

Details: jQuery < 1.9.0 XSS Vulnerability

OID: 1.3.6.1.4.1.25623.1.0.141636

... continues on next page ...

... continued from previous page ...
Version used: 2023-07-14T05:06:08Z
References
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2025-1803
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590

Medium (CVSS: 6.0)
NVT: TWiki CSRF Vulnerability
Summary TWiki is prone to a cross-site request forgery (CSRF) vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Installed version: 01.Feb.2003 Fixed version: 4.3.1
Impact Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.
Solution: Solution type: VendorFix Upgrade to version 4.3.1 or later.
Affected Software/OS TWiki version prior to 4.3.1
Vulnerability Insight Remote authenticated user can create a specially crafted image tag that, when viewed by the target user, will update pages on the target system with the privileges of the target user via HTTP requests.
Vulnerability Detection Method Details: TWiki CSRF Vulnerability OID:1.3.6.1.4.1.25623.1.0.800400
... continues on next page ...

... continued from previous page ...
Version used: 2024-06-28T05:05:33Z
References
cve: CVE-2009-1339 url: http://secunia.com/advisories/34880 url: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258 url: http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-diff--cve-2009-1339.txt

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled
Summary The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.
Quality of Detection (QoD): 99%
Vulnerability Detection Result The web server has the following HTTP methods enabled: TRACE
Impact An attacker may use this flaw to trick your legitimate web users to give him their credentials.
Solution: Solution type: Mitigation Disable the TRACE and TRACK methods in your web server configuration. Please see the manual of your web server or the references for more information.
Affected Software/OS Web servers with enabled TRACE and/or TRACK methods.
Vulnerability Insight It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.
Vulnerability Detection Method Checks if HTTP methods such as TRACE and TRACK are enabled and can be used. Details: HTTP Debugging Methods (TRACE/TRACK) Enabled OID:1.3.6.1.4.1.25623.1.0.11213 Version used: 2023-08-01T13:29:10Z
References
... continues on next page ...

... continued from previous page ...

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

Medium (CVSS: 5.3)

NVT: phpinfo() Output Reporting (HTTP)

Summary

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

The following files are calling the function `phpinfo()` which disclose potentially sensitive information:

<http://192.168.220.129/mutillidae/phpinfo.php>

... continues on next page ...

<p>... continued from previous page ...</p> <pre> Concluded from: <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX, NOFOLLOW, NOARCHIV ↪E" /></head> <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph ↪p5/cgi </td></tr> <h2>PHP Core</h2> <h2>PHP Variables</h2> http://192.168.220.129/phpinfo.php Concluded from: <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX, NOFOLLOW, NOARCHIV ↪E" /></head> <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph ↪p5/cgi </td></tr> <h2>PHP Core</h2> <h2>PHP Variables</h2></pre>
<p>Impact</p> <p>Some of the information that can be gathered from this file includes:</p> <p>The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.</p>
<p>Solution:</p> <p>Solution type: Workaround</p> <p>Delete the listed files or restrict access to them.</p>
<p>Affected Software/OS</p> <p>All systems exposing a file containing the output of the phpinfo() PHP function.</p> <p>This VT is also reporting if an affected endpoint for the following products have been identified:</p> <ul style="list-style-type: none"> - CVE-2008-0149: TUTOS - CVE-2023-49282, CVE-2023-49283: Microsoft Graph PHP SDK - CVE-2024-10486: Google for WooCommerce plugin for WordPress
<p>Vulnerability Insight</p> <p>Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory.</p>
<p>Vulnerability Detection Method</p> <p>This script reports files identified by the following separate VT: 'phpinfo() Output Detection (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.108474).</p> <p>Details: <code>phpinfo() Output Reporting (HTTP)</code> OID:1.3.6.1.4.1.25623.1.0.11229</p> <p>Version used: 2025-07-09T05:43:50Z</p>
<p>References</p> <p>cve: CVE-2008-0149</p>
<p>... continues on next page ...</p>

<p>cve: CVE-2023-49282 cve: CVE-2023-49283 cve: CVE-2024-10486 url: https://www.php.net/manual/en/function.phpinfo.php url: https://beaglesecurity.com/blog/vulnerability/revealing-phpinfo.html</p>	... continued from previous page ...
--	--------------------------------------

<p>Medium (CVSS: 5.0)</p>

<p>NVT: /doc directory browsable</p>

<h3>Summary</h3>

<p>The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.</p>
--

<h3>Quality of Detection (QoD): 80%</h3>
--

<h4>Vulnerability Detection Result</h4>

<p>Vulnerable URL: http://192.168.220.129/doc/</p>
--

<h4>Solution:</h4>

<p>Solution type: Mitigation</p>

<p>Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf:</p>
--

<pre><Directory /usr/doc> AllowOverride None order deny, allow deny from all allow from localhost </Directory></pre>
--

<h4>Vulnerability Detection Method</h4>

<p>Details: /doc directory browsable</p>
--

<p>OID:1.3.6.1.4.1.25623.1.0.10056</p>
--

<p>Version used: 2023-08-01T13:29:10Z</p>

<h4>References</h4>

<p>cve: CVE-1999-0678</p>

<p>url: http://www.securityfocus.com/bid/318</p>

<p>Medium (CVSS: 5.0)</p>

<p>NVT: QWikiwiki directory traversal vulnerability</p>

<h3>Summary</h3>

<p>The remote host is running QWikiwiki, a Wiki application written in PHP.</p>

<p>The remote version of this software contains a validation input flaw which may allow an attacker to use it to read arbitrary files on the remote host with the privileges of the web server.</p>

<p>... continues on next page ...</p>

. . . continued from previous page . . .
Quality of Detection (QoD): 99%
Vulnerability Detection Result Vulnerable URL: http://192.168.220.129/mutillidae/index.php?page=../../../../../../../../etc/passwd%00
Solution: Solution type: WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
Vulnerability Detection Method Details: QWikiwiki directory traversal vulnerability OID:1.3.6.1.4.1.25623.1.0.16100 Version used: 2025-04-15T05:54:49Z
References cve: CVE-2005-0283 url: http://www.securityfocus.com/bid/12163

Medium (CVSS: 5.0) NVT: awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check
Summary awiki is prone to multiple local file include (LFI) vulnerabilities because it fails to properly sanitize user-supplied input.
Quality of Detection (QoD): 99%
Vulnerability Detection Result Vulnerable URL: http://192.168.220.129/mutillidae/index.php?page=/etc/passwd
Impact An attacker can exploit this vulnerability to obtain potentially sensitive information and execute arbitrary local scripts in the context of the webserver process. This may allow the attacker to compromise the application and the host.
Solution: Solution type: WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
... continues on next page ...

<p style="text-align: right;">... continued from previous page ...</p> <hr/> <p>Affected Software/OS awiki version 20100125 and prior.</p> <hr/> <p>Vulnerability Detection Method Sends a crafted HTTP GET request and checks the response. Details: awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check OID:1.3.6.1.4.1.25623.1.0.103210 Version used: 2025-04-15T05:54:49Z</p> <hr/> <p>References url: https://www.exploit-db.com/exploits/36047/ url: http://www.securityfocus.com/bid/49187</p>

<p>Medium (CVSS: 4.8)</p> <p>NVT: Cleartext Transmission of Sensitive Information via HTTP</p> <hr/> <p>Summary The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.</p> <hr/> <p>Quality of Detection (QoD): 80%</p> <hr/> <p>Vulnerability Detection Result The following input fields were identified (URL:input name): http://192.168.220.129/dvwa/login.php:password http://192.168.220.129/phpMyAdmin/:pma_password http://192.168.220.129/phpMyAdmin/?D=A:pma_password http://192.168.220.129/tikiwiki/tiki-install.php:pass http://192.168.220.129/twiki/bin/view/TWiki/TWikiUserAuthentication:oldpassword</p> <hr/> <p>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.</p> <hr/> <p>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.</p> <hr/> <p>Affected Software/OS</p>
... continues on next page ...

<p>... continued from previous page ...</p> <p>Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.</p> <p>Vulnerability Detection Method</p> <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 OID:1.3.6.1.4.1.25623.1.0.108440 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 url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure url: https://cwe.mitre.org/data/definitions/319.html</p>

Medium (CVSS: 4.3) NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability
<p>Summary phpMyAdmin is prone to a cross-site scripting (XSS) vulnerability.</p>
<p>Quality of Detection (QoD): 99%</p>
<p>Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p>Impact Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.</p>
<p>Solution: Solution type: WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.</p>
<p>Affected Software/OS phpMyAdmin version 3.3.8.1 and prior.</p>
<p>Vulnerability Insight</p>
<p>... continues on next page ...</p>

... continued from previous page ...
The flaw is caused by input validation errors in the 'error.php' script when processing crafted BBcode tags containing '@' characters, which could allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.
Vulnerability Detection Method Details: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability OID:1.3.6.1.4.1.25623.1.0.801660 Version used: 2023-10-17T05:05:34Z
References cve: CVE-2010-4480 url: http://www.exploit-db.com/exploits/15699/ url: http://www.vupen.com/english/advisories/2010/3133 dfn-cert: DFN-CERT-2011-0467 dfn-cert: DFN-CERT-2011-0451 dfn-cert: DFN-CERT-2011-0016 dfn-cert: DFN-CERT-2011-0002

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
Product detection result cpe:/a:apache:http_server:2.2.8 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1 → .0.117232)
Summary Apache HTTP Server is prone to a cookie information disclosure vulnerability.
Quality of Detection (QoD): 99%
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.
Solution: Solution type: VendorFix Update to Apache HTTP Server version 2.2.22 or later.
Affected Software/OS ... continues on next page ...

... continued from previous page ...
Apache HTTP Server versions 2.2.0 through 2.2.21.
Vulnerability Insight The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.
Vulnerability Detection Method Details: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability OID:1.3.6.1.4.1.25623.1.0.902830 Version used: 2025-03-05T05:38:53Z
Product Detection Result Product: cpe:/a:apache:http_server:2.2.8 Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)
References cve: CVE-2012-0053 url: http://secunia.com/advisories/47779 url: http://www.securityfocus.com/bid/51706 url: http://www.exploit-db.com/exploits/18442 url: http://rhn.redhat.com/errata/RHSA-2012-0128.html url: http://httpd.apache.org/security/vulnerabilities_22.html url: http://svn.apache.org/viewvc?view=revision&revision=1235454 url: http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html cert-bund: CB-K15/0080 cert-bund: CB-K14/1505 cert-bund: CB-K14/0608 dfn-cert: DFN-CERT-2015-0082 dfn-cert: DFN-CERT-2014-1592 dfn-cert: DFN-CERT-2014-0635 dfn-cert: DFN-CERT-2013-1307 dfn-cert: DFN-CERT-2012-1276 dfn-cert: DFN-CERT-2012-1112 dfn-cert: DFN-CERT-2012-0928 dfn-cert: DFN-CERT-2012-0758 dfn-cert: DFN-CERT-2012-0744 dfn-cert: DFN-CERT-2012-0568 dfn-cert: DFN-CERT-2012-0425 dfn-cert: DFN-CERT-2012-0424 dfn-cert: DFN-CERT-2012-0387 dfn-cert: DFN-CERT-2012-0343 dfn-cert: DFN-CERT-2012-0332 dfn-cert: DFN-CERT-2012-0306 dfn-cert: DFN-CERT-2012-0264 dfn-cert: DFN-CERT-2012-0203
... continues on next page ...

	... continued from previous page ...
dfn-cert: DFN-CERT-2012-0188	
Medium (CVSS: 4.3)	
NVT: jQuery < 1.6.3 XSS Vulnerability	
Summary jQuery is prone to a cross-site scripting (XSS) vulnerability.	
Quality of Detection (QoD): 80%	
Vulnerability Detection Result Installed version: 1.3.2 Fixed version: 1.6.3 Installation path / port: /mutillidae/javascript/ddsmoothmenu/jquery.min.js Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info): - Identified file: http://192.168.220.129/mutillidae/javascript/ddsmoothmenu/jquery.min.js - Referenced at: http://192.168.220.129/mutillidae/	
Solution: Solution type: VendorFix Update to version 1.6.3 or later.	
Affected Software/OS jQuery prior to version 1.6.3.	
Vulnerability Insight Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: jQuery < 1.6.3 XSS Vulnerability OID:1.3.6.1.4.1.25623.1.0.141637 Version used: 2023-07-14T05:06:08Z	
References cve: CVE-2011-4969 url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/ cert-bund: CB-K17/0195 dfn-cert: DFN-CERT-2017-0199 dfn-cert: DFN-CERT-2016-0890	

[[return to 192.168.220.129](http://192.168.220.129)]

2.1.11 Medium 25/tcp

Medium (CVSS: 6.8) NVT: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability
Summary Multiple vendors' implementations of 'STARTTLS' are prone to a vulnerability that lets attackers inject arbitrary commands.
Quality of Detection (QoD): 99%
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact An attacker can exploit this issue to execute arbitrary commands in the context of the user running the application. Successful exploits can allow attackers to obtain email usernames and passwords.
Solution: Solution type: VendorFix Updates are available. Please see the references for more information.
Affected Software/OS The following vendors are known to be affected: Ipswitch Kerio Postfix Qmail-TLS Oracle SCO Group spamdyke ISC
Vulnerability Detection Method Send a special crafted 'STARTTLS' request and check the response. Details: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection . ↔.. OID:1.3.6.1.4.1.25623.1.0.103935 Version used: 2023-10-31T05:06:37Z
References cve: CVE-2011-0411 cve: CVE-2011-1430 ... continues on next page ...

... continued from previous page ...

```
cve: CVE-2011-1431
cve: CVE-2011-1432
cve: CVE-2011-1506
cve: CVE-2011-1575
cve: CVE-2011-1926
cve: CVE-2011-2165
url: http://www.securityfocus.com/bid/46767
url: http://kolab.org/pipermail/kolab-announce/2011/000101.html
url: http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424
url: http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7
url: http://www.kb.cert.org/vuls/id/MAPG-8D9M4P
url: http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-no
→tes.txt
url: http://www.postfix.org/CVE-2011-0411.html
url: http://www.pureftpd.org/project/pure-ftpd/news
url: http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNotes
→_XCS_9_1_1/EN_ReleaseNotes_WG_XCS_9_1_TLS_Hotfix.pdf
url: http://www.spamdyke.org/documentation/Changelog.txt
url: http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?include
→_text=1
url: http://www.securityfocus.com/archive/1/516901
url: http://support.avaya.com/css/P8/documents/100134676
url: http://support.avaya.com/css/P8/documents/100141041
url: http://www.oracle.com/technetwork/topics/security/cpupapr2011-301950.html
url: http://inoa.net/qmail-tls/vu555316.patch
url: http://www.kb.cert.org/vuls/id/555316
cert-bund: CB-K15/1514
dfn-cert: DFN-CERT-2011-0917
dfn-cert: DFN-CERT-2011-0912
dfn-cert: DFN-CERT-2011-0897
dfn-cert: DFN-CERT-2011-0844
dfn-cert: DFN-CERT-2011-0818
dfn-cert: DFN-CERT-2011-0808
dfn-cert: DFN-CERT-2011-0771
dfn-cert: DFN-CERT-2011-0741
dfn-cert: DFN-CERT-2011-0712
dfn-cert: DFN-CERT-2011-0673
dfn-cert: DFN-CERT-2011-0597
dfn-cert: DFN-CERT-2011-0596
dfn-cert: DFN-CERT-2011-0519
dfn-cert: DFN-CERT-2011-0516
dfn-cert: DFN-CERT-2011-0483
dfn-cert: DFN-CERT-2011-0434
dfn-cert: DFN-CERT-2011-0393
dfn-cert: DFN-CERT-2011-0381
```

<p>Medium (CVSS: 5.9)</p> <p>NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection</p>
<p>Product detection result cpe:/a:ietf:transport_layer_security:1.0 Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)</p>
<p>Summary It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.</p>
<p>Quality of Detection (QoD): 98%</p>
<p>Vulnerability Detection Result In addition to TLSv1.0+ the service is also providing the deprecated SSLv2 and S ↔SLv3 protocols and supports one or more ciphers. Those supported ciphers can b ↔e found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.256 ↔23.1.0.802067) 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 SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more resources supporting you with this task.</p>
<p>Affected Software/OS All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.</p>
<p>Vulnerability Insight The SSLv2 and SSLv3 protocols contain known cryptographic flaws like: - CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE) - CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)</p>
<p>Vulnerability Detection Method Checks the used SSL protocols of the services provided by this system. Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.111012</p>
<p>... continues on next page ...</p>

	... continued from previous page ...
Version used:	2025-03-27T05:38:50Z
Product Detection Result	
Product:	cpe:/a:ietf:transport_layer_security:1.0
Method:	SSL/TLS: Version Detection
OID:	1.3.6.1.4.1.25623.1.0.105782)
References	
cve:	CVE-2016-0800
cve:	CVE-2014-3566
url:	https://ssl-config.mozilla.org
url:	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html
url:	https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html
url:	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html
url:	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindesstandard_BSI_TLS_Version_2_4.html
url:	https://web.archive.org/web/20240113175943/https://www.bettercrypto.org
url:	https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
url:	https://drownattack.com
url:	https://www.imperialviolet.org/2014/10/14/poodle.html
cert-bund:	WID-SEC-2025-1658
cert-bund:	WID-SEC-2023-0431
cert-bund:	WID-SEC-2023-0427
cert-bund:	CB-K18/0094
cert-bund:	CB-K17/1198
cert-bund:	CB-K17/1196
cert-bund:	CB-K16/1828
cert-bund:	CB-K16/1438
cert-bund:	CB-K16/1384
cert-bund:	CB-K16/1141
cert-bund:	CB-K16/1107
cert-bund:	CB-K16/1102
cert-bund:	CB-K16/0792
cert-bund:	CB-K16/0599
cert-bund:	CB-K16/0597
cert-bund:	CB-K16/0459
cert-bund:	CB-K16/0456
cert-bund:	CB-K16/0433
cert-bund:	CB-K16/0424
cert-bund:	CB-K16/0415
cert-bund:	CB-K16/0413
cert-bund:	CB-K16/0374
... continues on next page ...	

... continued from previous page ...

cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354

Medium (CVSS: 5.3)

NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

Summary

| ... continues on next page ...

<p>... continued from previous page ...</p> <p>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.</p> <p>Quality of Detection (QoD): 80%</p> <p>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:00FAF93A4C7FB6B9CC:1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D →626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for C →omplication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no su →ch thing outside US,C=XX (Server certificate)</p> <p>Impact Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.</p> <p>Solution: Solution type: Mitigation Replace the certificate with a stronger key and reissue the certificates it signed.</p> <p>Vulnerability Insight SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.</p> <p>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</p> <p>References url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf</p>

Medium (CVSS: 5.0)

NVT: SSL/TLS: Certificate Expired

Product detection result

cpe:/a:ietf:transport_layer_security

Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
 →623.1.0.103692)

... continues on next page ...

	... continued from previous page ...
Summary	The remote server's SSL/TLS certificate has already expired.
Quality of Detection (QoD): 99%	
Vulnerability Detection Result	<p>The certificate of the remote service expired on 2010-04-16 14:07:45.</p> <p>Certificate details:</p> <pre> fingerprint (SHA-1) ED093088706603BFD5DC237399B498DA2D4D31C6 fingerprint (SHA-256) E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A ↪F1E32DEE436DE813CC issued by 1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is ↪ no such thing outside US,C=XX public key algorithm RSA public key size (bits) 1024 serial 00FAF93A4C7FB6B9CC signature algorithm sha1WithRSAEncryption subject 1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is ↪ no such thing outside US,C=XX subject alternative names (SAN) None valid from 2010-03-17 14:07:45 UTC valid until 2010-04-16 14:07:45 UTC </pre>
Solution:	<p>Solution type: Mitigation</p> <p>Replace the SSL/TLS certificate by a new one.</p>
Vulnerability Insight	<p>This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.</p>
Vulnerability Detection Method	<p>Details: SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: 2024-06-14T05:05:48Z</p>
Product Detection Result	<p>Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Collect and Report Certificate Details OID: 1.3.6.1.4.1.25623.1.0.103692)</p>

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 (QoD): 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)
Summary The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 70%
Vulnerability Detection Result The following indicates that the remote SSL/TLS service is affected: Protocol Version Successful re-done SSL/TLS handshakes (Renegotiation) over an → existing / already established SSL/TLS connection ... continues on next page ...

		... continued from previous page ...
<hr/>		<hr/>
TLSv1.0 10		
Impact		
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.		
Solution:		
Solution type: VendorFix		
Users should contact their vendors for specific patch information.		
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.		
Affected Software/OS		
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.		
Vulnerability Insight		
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.		
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:		
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.		
Both CVEs are still kept in this VT as a reference to the origin of this flaw.		
Vulnerability Detection Method		
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.		
Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)		
OID:1.3.6.1.4.1.25623.1.0.117761		
Version used: 2024-09-27T05:05:23Z		
References		
cve: CVE-2011-1473		
cve: CVE-2011-5094		
url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego-tiation-dos/		
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/		
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation		
url: https://www.openwall.com/lists/oss-security/2011/07/08/2		
cert-bund: WID-SEC-2024-1591		
cert-bund: WID-SEC-2024-0796		
cert-bund: WID-SEC-2023-1435		
cert-bund: CB-K17/0980		
cert-bund: CB-K17/0979		
... continues on next page ...		

... continued from previous page ...

cert-bund: CB-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2025-0933
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112

Medium (CVSS: 4.3)

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

Product detection result

cpe:/a:ietf:transport_layer_security:1.0

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

Summary

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result

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

Impact

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

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

Solution:

Solution type: Mitigation

It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols.

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

Affected Software/OS

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

... continues on next page ...

<p>... continued from previous page ...</p> <ul style="list-style-type: none"> - CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder - CVE-2024-41270: Gorush v1.18.4 - CVE-2025-3200: Multiple products from Wiesemann & Theis
<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>Checks the used TLS protocols of the services provided by this system.</p> <p>Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274</p> <p>Version used: 2025-04-30T05:39:51Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:ietf:transport_layer_security:1.0 Method: SSL/TLS: Version Detection OID: 1.3.6.1.4.1.25623.1.0.105782)</p>
<p>References</p> <p>cve: CVE-2011-3389 cve: CVE-2015-0204 cve: CVE-2023-41928 cve: CVE-2024-41270 cve: CVE-2025-3200 url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindesstandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters--report-2014 url: https://datatracker.ietf.org/doc/rfc8996/ url: https://vhacker.blogspot.com/2011/09/beast.html url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak url: https://certvde.com/en/advisories/VDE-2025-031/ url: https://gist.github.com/nyxfqq/cfae38fada582a0f576d154be1aeb1fc url: https://advisories.ncsc.nl/advisory?id=NCSC-2024-0273 cert-bund: WID-SEC-2023-1435</p>
... continues on next page ...

... continued from previous page ...

cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738

... continues on next page ...

... continued from previous page ...
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
Product detection result cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.→802067)
Summary This host is accepting 'RSA_EXPORT' cipher suites and is prone to a man-in-the-middle (MITM) vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result 'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5 'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5
Impact Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.
Solution: Solution type: VendorFix - Remove support for 'RSA_EXPORT' cipher suites from the service. Please see the references for more resources supporting you with this task. - If the service is using OpenSSL: Update to version 0.9.8zd, 1.0.0p, 1.0.1k or later.
... continues on next page ...

... continued from previous page ...

Affected Software/OS

- Hosts accepting 'RSA_EXPORT' cipher suites.
- OpenSSL versions prior to 0.9.8zd, 1.0.0 prior to 1.0.0p and 1.0.1 prior to 1.0.1k.

Vulnerability Insight

Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

Vulnerability Detection Method

Checks previous collected cipher suites.

Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

OID:1.3.6.1.4.1.25623.1.0.805142

Version used: 2025-03-27T05:38:50Z

Product Detection Result

Product: cpe:/a:ietf:transport_layer_security

Method: SSL/TLS: Report Supported Cipher Suites

OID: 1.3.6.1.4.1.25623.1.0.802067)

References

cve: CVE-2015-0204

url: <https://freakattack.com>

url: <https://openssl-library.org/news/secadv/20150108.txt>

url: <https://web.archive.org/web/20210122095002/http://www.securityfocus.com/bid/71936>

url: <https://www.secpod.com/blog/freak-attack>

url: <https://blog.cryptographyengineering.com/2015/03/03/attack-of-week-freak-or-factoring-nsa>

url: <https://ssl-config.mozilla.org>

url: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html>

url: https://www.bsi.bund.de/EN/Themen/Offentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html

url: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html>

url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindesstandard_BSI_TLS_Version_2_4.html

url: <https://web.archive.org/web/20240113175943/https://www.bettercrypto.org>

url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014>

cert-bund: CB-K18/0799

cert-bund: CB-K16/1289

cert-bund: CB-K16/1096

cert-bund: CB-K15/1751

... continues on next page ...

cert-bund: CB-K15/1266 cert-bund: CB-K15/0850 cert-bund: CB-K15/0764 cert-bund: CB-K15/0720 cert-bund: CB-K15/0548 cert-bund: CB-K15/0526 cert-bund: CB-K15/0509 cert-bund: CB-K15/0493 cert-bund: CB-K15/0384 cert-bund: CB-K15/0365 cert-bund: CB-K15/0364 cert-bund: CB-K15/0302 cert-bund: CB-K15/0192 cert-bund: CB-K15/0016 dfn-cert: DFN-CERT-2018-1408 dfn-cert: DFN-CERT-2016-1372 dfn-cert: DFN-CERT-2016-1164 dfn-cert: DFN-CERT-2016-0388 dfn-cert: DFN-CERT-2015-1853 dfn-cert: DFN-CERT-2015-1332 dfn-cert: DFN-CERT-2015-0884 dfn-cert: DFN-CERT-2015-0800 dfn-cert: DFN-CERT-2015-0758 dfn-cert: DFN-CERT-2015-0567 dfn-cert: DFN-CERT-2015-0544 dfn-cert: DFN-CERT-2015-0530 dfn-cert: DFN-CERT-2015-0396 dfn-cert: DFN-CERT-2015-0375 dfn-cert: DFN-CERT-2015-0374 dfn-cert: DFN-CERT-2015-0305 dfn-cert: DFN-CERT-2015-0199 dfn-cert: DFN-CERT-2015-0021	... continued from previous page ...
--	--------------------------------------

Medium (CVSS: 4.0)

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

Summary

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

Quality of Detection (QoD): 80%
--

Vulnerability Detection Result

Server Temporary Key Size: 1024 bits

Impact

... continues on next page ...

... continued from previous page ...
An attacker might be able to decrypt the SSL/TLS communication offline.
<p>Solution:</p> <p>Solution type: Workaround</p> <ul style="list-style-type: none"> - Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. Please see the references for more resources supporting you with this task. - 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>Affected Software/OS</p> <p>All services providing an encrypted communication using Diffie-Hellman groups with insufficient strength.</p>
<p>Vulnerability Insight</p> <p>The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.</p>
<p>Vulnerability Detection Method</p> <p>Checks the DHE temporary public key size.</p> <p>Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability ↔.. OID:1.3.6.1.4.1.25623.1.0.106223 Version used: 2025-03-27T05:38:50Z</p>
<p>References</p> <p>url: https://weakdh.org url: https://weakdh.org/sysadmin.html url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014 url: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslcertificatefile</p>

Medium (CVSS: 4.0) NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
<p>Summary The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173 →652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic →ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi →ng outside US,C=XX Signature Algorithm: sha1WithRSAEncryption</p>
<p>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.</p>
<p>Vulnerability Insight The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use: - Secure Hash Algorithm 1 (SHA-1) - Message Digest 5 (MD5) - Message Digest 4 (MD4) - Message Digest 2 (MD2) Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates. NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive: Fingerprint1 or fingerprint1, Fingerprint2</p>
<p>Vulnerability Detection Method Check which hashing algorithm was used to sign the remote SSL/TLS certificate. Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm OID:1.3.6.1.4.1.25623.1.0.105880</p>
... continues on next page ...

... continued from previous page ...
Version used: 2021-10-15T11:13:32Z
References url: sha-1-based-signature-algorithms/">https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with->sha-1-based-signature-algorithms/
[return to 192.168.220.129]

2.1.12 Medium 5432/tcp

Medium (CVSS: 5.9) NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
Product detection result cpe:/a:ietf:transport_layer_security:1.0 Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
Summary It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.
Quality of Detection (QoD): 98%
Vulnerability Detection Result In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020->67) VT.
Impact An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.
Solution: Solution type: Mitigation It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more resources supporting you with this task.
... continues on next page ...

	... continued from previous page ...
Affected Software/OS	All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.
Vulnerability Insight	<p>The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:</p> <ul style="list-style-type: none"> - CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE) - CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)
Vulnerability Detection Method	<p>Checks the used SSL protocols of the services provided by this system.</p> <p>Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.111012 Version used: 2025-03-27T05:38:50Z</p>
Product Detection Result	<p>Product: cpe:/a:ietf:transport_layer_security:1.0 Method: SSL/TLS: Version Detection OID: 1.3.6.1.4.1.25623.1.0.105782)</p>
References	<p>cve: CVE-2016-0800 cve: CVE-2014-3566 url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014 url: https://drownattack.com url: https://www.imperialviolet.org/2014/10/14/poodle.html cert-bund: WID-SEC-2025-1658 cert-bund: WID-SEC-2023-0431 cert-bund: WID-SEC-2023-0427 cert-bund: CB-K18/0094 cert-bund: CB-K17/1198 cert-bund: CB-K17/1196 cert-bund: CB-K16/1828 cert-bund: CB-K16/1438 cert-bund: CB-K16/1384 cert-bund: CB-K16/1141</p>
	... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/1107
cert-bund: CB-K16/1102
cert-bund: CB-K16/0792
cert-bund: CB-K16/0599
cert-bund: CB-K16/0597
cert-bund: CB-K16/0459
cert-bund: CB-K16/0456
cert-bund: CB-K16/0433
cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354

Medium (CVSS: 5.9)

NVT: SSL/TLS: Report Weak Cipher Suites

Product detection result

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

Summary

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result

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

TLS_RSA_WITH_RC4_128_SHA

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

TLS_RSA_WITH_RC4_128_SHA

Impact

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

Solution:

Solution type: Mitigation

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

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

Affected Software/OS

All services providing an encrypted communication using weak SSL/TLS cipher suites.

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

... continues on next page ...

... continued from previous page ...
- 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 Checks previous collected cipher suites. 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. Details: SSL/TLS: Report Weak Cipher Suites OID:1.3.6.1.4.1.25623.1.0.103440 Version used: 2025-03-27T05:38:50Z
Product Detection Result Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Report Supported Cipher Suites OID: 1.3.6.1.4.1.25623.1.0.802067)
References cve: CVE-2013-2566 cve: CVE-2015-2808 cve: CVE-2015-4000 url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindesstandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014 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
... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101

... continues on next page ...

... continued from previous page ...

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

Medium (CVSS: 5.3)

NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

Summary

The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

... continues on next page ...

<p>... continued from previous page ...</p> <p>The remote SSL/TLS server is using the following certificate(s) with a RSA key w ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer): 1024:RSA:00FAF93A4C7FB6B9CC:1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D →626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for C ompliation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no su ch thing outside US,C=XX (Server certificate)</p>
<p>Impact Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.</p>
<p>Solution: Solution type: Mitigation Replace the certificate with a stronger key and reissue the certificates it signed.</p>
<p>Vulnerability Insight SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.</p>
<p>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</p>
<p>References url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf</p>

<p>Medium (CVSS: 5.0)</p> <p>NVT: SSL/TLS: Certificate Expired</p>
<p>Product detection result cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25 →623.1.0.103692)</p>
<p>Summary The remote server's SSL/TLS certificate has already expired.</p>
<p>Quality of Detection (QoD): 99%</p>
<p>Vulnerability Detection Result ... continues on next page ...</p>

<p>... continued from previous page ...</p>	
<pre>The certificate of the remote service expired on 2010-04-16 14:07:45. Certificate details: fingerprint (SHA-1) ED093088706603BFD5DC237399B498DA2D4D31C6 fingerprint (SHA-256) E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A →F1E32DEE436DE813CC issued by 1.2.840.113549.1.9.1=#726F6F74407562756E747538 →30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office → for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is → no such thing outside US,C=XX public key algorithm RSA public key size (bits) 1024 serial 00FAF93A4C7FB6B9CC signature algorithm sha1WithRSAEncryption subject 1.2.840.113549.1.9.1=#726F6F74407562756E747538 →30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office → for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is → no such thing outside US,C=XX subject alternative names (SAN) None valid from 2010-03-17 14:07:45 UTC valid until 2010-04-16 14:07:45 UTC</pre>	
Solution: Solution type: Mitigation Replace the SSL/TLS certificate by a new one.	
Vulnerability Insight This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.	
Vulnerability Detection Method Details: SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: 2024-06-14T05:05:48Z	
Product Detection Result Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Collect and Report Certificate Details OID: 1.3.6.1.4.1.25623.1.0.103692)	

Medium (CVSS: 5.0)

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

Summary

... continues on next page ...

... continued from previous page ...	
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.	
Quality of Detection (QoD): 70%	
<p>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 </p>	
<p>Impact The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.</p>	
<p>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.</p>	
<p>Affected Software/OS Every SSL/TLS service which does not properly restrict client-initiated renegotiation.</p>	
<p>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.</p>	
<p>Vulnerability Detection Method Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection. Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) OID:1.3.6.1.4.1.25623.1.0.117761 Version used: 2024-09-27T05:05:23Z </p>	
<p>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 ... </p>	

... continued from previous page ...

url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
url: <https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation>
url: <https://www.openwall.com/lists/oss-security/2011/07/08/2>
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-0796
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K17/0980
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2025-0933
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112

Medium (CVSS: 4.3)

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

Product detection result

cpe:/a:ietf:transport_layer_security:1.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

Summary

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result

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

Impact

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

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

Solution:

... continues on next page ...

... continued from previous page ...

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 resources supporting you with this task.

Affected Software/OS

- All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols
- CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder
- CVE-2024-41270: Gorush v1.18.4
- CVE-2025-3200: Multiple products from Wiesemann & Theis

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

Checks 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: 2025-04-30T05:39:51Z

Product Detection Result

Product: cpe:/a:ietf:transport_layer_security:1.0

Method: SSL/TLS: Version Detection

OID: 1.3.6.1.4.1.25623.1.0.105782)

References

cve: CVE-2011-3389

cve: CVE-2015-0204

cve: CVE-2023-41928

cve: CVE-2024-41270

cve: CVE-2025-3200

url: <https://ssl-config.mozilla.org>

url: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html>

url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html

url: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html>

url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html

url: <https://web.archive.org/web/20240113175943/https://www.bettercrypto.org>

url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters>

... continues on next page ...

... continued from previous page ...

↔-report-2014
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://certvde.com/en/advisories/VDE-2025-031/>
url: <https://gist.github.com/nyxfqq/cfae38fada582a0f576d154be1aeb1fc>
url: <https://advisories.ncsc.nl/advisory?id=NCSC-2024-0273>
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047

... continues on next page ...

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

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

	Medium (CVSS: 4.0)
--	--------------------

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

	Summary
--	----------------

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

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

	Vulnerability Detection Result
--	---------------------------------------

	Server Temporary Key Size: 1024 bits
--	--------------------------------------

	Impact
--	---------------

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

	Solution:
--	------------------

	Solution type: Workaround
--	----------------------------------

- | | |
|--|--|
| | <ul style="list-style-type: none"> - Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. Please see the references for more resources supporting you with this task. - 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. |
|--|--|

	Affected Software/OS
--	-----------------------------

	All services providing an encrypted communication using Diffie-Hellman groups with insufficient strength.
--	---

	Vulnerability Insight
--	------------------------------

	... continues on next page ...
--	--------------------------------

... continued from previous page ...
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: 2025-03-27T05:38:50Z
References url: https://weakdh.org url: https://weakdh.org/sysadmin.html url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindesstandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014 url: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslcertificatefile

Medium (CVSS: 4.0)

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

Summary

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

Quality of Detection (QoD): 80%
--

Vulnerability Detection Result

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

Subject: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173 →652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX
--

... continues on next page ...

<p>... continued from previous page ...</p> <p>Signature Algorithm: sha1WithRSAEncryption</p> <p>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.</p> <p>Vulnerability Insight The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use: - Secure Hash Algorithm 1 (SHA-1) - Message Digest 5 (MD5) - Message Digest 4 (MD4) - Message Digest 2 (MD2) Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates. NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive: Fingerprint1 or fingerprint1, Fingerprint2</p> <p>Vulnerability Detection Method Check which hashing algorithm was used to sign the remote SSL/TLS certificate. Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm OID:1.3.6.1.4.1.25623.1.0.105880 Version used: 2021-10-15T11:13:32Z</p> <p>References url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/</p>

[[return to 192.168.220.129](#)]

2.1.13 Medium 21/tcp

Medium (CVSS: 6.4)
NVT: Anonymous FTP Login Reporting
Summary
... continues on next page ...

<p>... continued from previous page ...</p> <p>Reports if the remote FTP Server allows anonymous logins.</p> <p>Quality of Detection (QoD): 80%</p> <p>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</p> <p>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.</p> <p>Solution: Solution type: Mitigation If you do not want to share files, you should disable anonymous logins.</p> <p>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.</p> <p>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</p> <p>References cve: CVE-1999-0497</p>
--

Medium (CVSS: 4.8)

NVT: FTP Unencrypted Cleartext Login

Summary

... continues on next page ...

<p>... continued from previous page ...</p> <p>The remote host is running a FTP service that allows cleartext logins over unencrypted connections.</p> <p>Quality of Detection (QoD): 70%</p> <p>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.</p> <p>Impact An attacker can uncover login names and passwords by sniffing traffic to the FTP service.</p> <p>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.</p> <p>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</p>

[[return to 192.168.220.129](#)]

2.1.14 Medium 5900/tcp

<p>Medium (CVSS: 4.8)</p> <p>NVT: VNC Server Unencrypted Data Transmission</p>
<p>Summary The remote host is running a VNC server providing one or more insecure or cryptographically weak Security Type(s) not intended for use on untrusted networks.</p>
<p>Quality of Detection (QoD): 70%</p> <p>Vulnerability Detection Result The VNC server provides the following insecure or cryptographically weak Security Type(s): ... continues on next page ...</p>

	... continued from previous page ...
2 (VNC authentication)	
Impact	An attacker can uncover sensitive data by sniffing traffic to the VNC server.
Solution:	
Solution type: Mitigation	Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254]. Some VNC server vendors are also providing more secure Security Types within their products.
Vulnerability Detection Method	
Details: VNC Server Unencrypted Data Transmission	
OID:1.3.6.1.4.1.25623.1.0.108529	
Version used: 2023-07-12T05:05:04Z	
References	
url: https://tools.ietf.org/html/rfc6143#page-10	

[[return to 192.168.220.129](#)]

2.1.15 Medium 23/tcp

Medium (CVSS: 4.8)
NVT: Telnet Unencrypted Cleartext Login
Summary
The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.
Quality of Detection (QoD): 70%
Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.
Impact
An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.
Solution:
Solution type: Mitigation
Replace Telnet with a protocol like SSH which supports encrypted connections.
Vulnerability Detection Method
... continues on next page ...

... continued from previous page ...

Details: Telnet Unencrypted Cleartext Login
OID:1.3.6.1.4.1.25623.1.0.108522
Version used: 2023-10-13T05:06:09Z

[[return to 192.168.220.129](#)]

2.1.16 Medium 2121/tcp

Medium (CVSS: 4.8)

NVT: FTP Unencrypted Cleartext Login

Summary

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

Quality of Detection (QoD): 70%

Vulnerability Detection Result

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

Non-anonymous sessions: 331 Password required for openvasvt

Anonymous sessions: 331 Password required for anonymous

Impact

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

Solution:

Solution type: Mitigation

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

Vulnerability Detection Method

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

Details: FTP Unencrypted Cleartext Login

OID:1.3.6.1.4.1.25623.1.0.108528

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

[[return to 192.168.220.129](#)]

2.1.17 Medium 445/tcp

Medium (CVSS: 6.0) NVT: Samba 3.0.0 <= 3.0.25rc3 MS-RPC Remote Shell Command Execution Vulnerability - Active Check
Product detection result cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
Summary Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.
Quality of Detection (QoD): 99%
Vulnerability Detection Result By sending a special crafted SMB request it was possible to execute ‘‘ping -p 5f ↪4f70656e564153565431313737385f -c50 192.168.220.128‘‘ on the remote host. Received answer (ICMP "Data" field): <pre>0x00: 38 79 24 69 2E AB 08 00 56 54 31 31 37 37 38 5F 8y\$i....VT11778_ 0x10: 5F 4F 70 65 6E 56 41 53 56 54 31 31 37 37 38 5F _OpenVASVT11778_ 0x20: 5F 4F 70 65 6E 56 41 53 56 54 31 31 37 37 38 5F _OpenVASVT11778_ 0x30: 5F 4F 70 65 6E 56 41 53 _OpenVAS</pre>
Impact An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application.
Solution: Solution type: VendorFix Updates are available. Please see the referenced vendor advisory.
Affected Software/OS Samba versions 3.0.0 through 3.0.25rc3.
Vulnerability Detection Method Sends a crafted SMB request and checks if the target is connecting back to the scanner host. Note: For a successful detection of this flaw the scanner host needs to be able to directly receive ICMP echo requests from the target. Details: Samba 3.0.0 <= 3.0.25rc3 MS-RPC Remote Shell Command Execution Vulnerability - . ↪.. OID:1.3.6.1.4.1.25623.1.0.108011 Version used: 2025-03-18T05:38:50Z
Product Detection Result
... continues on next page ...

<p>... continued from previous page ...</p> <p>Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)</p>
<p>References</p> <p>cve: CVE-2007-2447 url: https://www.samba.org/samba/security/CVE-2007-2447.html url: https://web.archive.org/web/20210121173708/http://www.securityfocus.com/bid/23972</p>

[[return to 192.168.220.129](#)]

2.1.18 Low 22/tcp

<p>Low (CVSS: 2.6)</p> <p>NVT: Weak MAC Algorithm(s) Supported (SSH)</p>
<p>Product detection result</p> <p>cpe:/a:ietf:secure_shell_protocol Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 →)</p>
<p>Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result The remote SSH server supports the following weak client-to-server MAC algorithm →(s): hmac-md5 hmac-md5-96 hmac-sha1-96 umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm →(s): hmac-md5 hmac-md5-96 hmac-sha1-96 umac-64@openssh.com</p>
<p>Solution: ... continues on next page ...</p>

<p style="text-align: right;">... continued from previous page ...</p> <p>Solution type: Mitigation Disable the reported weak MAC algorithm(s).</p> <p>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: 2024-06-14T05:05:48Z</p> <p>Product Detection Result Product: cpe:/a:ietf:secure_shell_protocol Method: SSH Protocol Algorithms Supported OID: 1.3.6.1.4.1.25623.1.0.105565)</p> <p>References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4</p>
--

[[return to 192.168.220.129](#)]

2.1.19 Low 25/tcp

<p>Low (CVSS: 3.7)</p> <p>NVT: SSL/TLS: 'DHE_EXPORT' MITM Security Bypass Vulnerability (LogJam)</p> <p>Product detection result cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.→802067)</p> <p>Summary This host is accepting 'DHE_EXPORT' cipher suites and is prone to a man-in-the-middle (MITM) vulnerability.</p> <p>Quality of Detection (QoD): 80%</p>
<p>... continues on next page ...</p>

... continued from previous page ...

Vulnerability Detection Result

'DHE_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5

Impact

Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Solution:

Solution type: VendorFix

- Remove support for 'DHE_EXPORT' cipher suites from the service. Please see the references for more resources supporting you with this task.
- If the service is using OpenSSL: Update to version 1.0.1n, 1.0.2b or later.

Affected Software/OS

- Hosts accepting 'DHE_EXPORT' cipher suites.
- OpenSSL versions prior to 1.0.1n and 1.0.2 prior to 1.0.2b.

Vulnerability Insight

Flaw is triggered when handling Diffie-Hellman key exchanges defined in the 'DHE_EXPORT' cipher suites.

Vulnerability Detection Method

Checks previous collected cipher suites.

Details: SSL/TLS: 'DHE_EXPORT' MITM Security Bypass Vulnerability (LogJam)

OID:1.3.6.1.4.1.25623.1.0.805188

Version used: 2025-03-27T05:38:50Z

Product Detection Result

Product: cpe:/a:ietf:transport_layer_security

Method: SSL/TLS: Report Supported Cipher Suites

OID: 1.3.6.1.4.1.25623.1.0.802067)

References

cve: CVE-2015-4000

url: <https://weakdh.org>

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

... continues on next page ...

... continued from previous page ...

url: <https://web.archive.org/web/20210122160144/http://www.securityfocus.com/bid/74733>
url: <https://weakdh.org/imperfect-forward-secrecy.pdf>
url: <https://openwall.com/lists/oss-security/2015/05/20/8>
url: <https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained>
url: <https://openssl-library.org/post/2015-05-20-logjam-freak-upcoming-changes/index.html>
url: <https://ssl-config.mozilla.org>
url: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html>
url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html
url: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html>
url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindesstandard_BSI_TLS_Version_2_4.html
url: <https://web.archive.org/web/20240113175943/https://www.bettercrypto.org>
url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014>
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
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-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
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-K15/0964
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-K15/0877
cert-bund: CB-K15/0834
cert-bund: CB-K15/0802
cert-bund: CB-K15/0733
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-2016-1692
dfn-cert: DFN-CERT-2016-1648
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-2015-1679
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-2015-1016
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-2015-0925
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0737

Low (CVSS: 3.4)

NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

... continues on next page ...

<p>... continued from previous page ...</p> <p>Product detection result cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0. ↳802067)</p> <p>Summary This host is prone to an information disclosure vulnerability.</p> <p>Quality of Detection (QoD): 80%</p> <p>Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.</p> <p>Impact Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.</p> <p>Solution: Solution type: Mitigation Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+</p> <p>Vulnerability Insight The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code</p> <p>Vulnerability Detection Method Evaluate previous collected information about this service. Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability . ↳.. OID:1.3.6.1.4.1.25623.1.0.802087 Version used: 2024-09-30T08:38:05Z</p> <p>Product Detection Result Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Report Supported Cipher Suites OID: 1.3.6.1.4.1.25623.1.0.802067)</p> <p>References cve: CVE-2014-3566 url: https://www.openssl.org/~bodo/ssl-poodle.pdf url: http://www.securityfocus.com/bid/70574</p>
... continues on next page ...

... continued from previous page ...

url: <https://www.imperialviolet.org/2014/10/14/poodle.html>
url: <https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html>
url: <http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin>
↪g-ssl-30.html
cert-bund: WID-SEC-2025-1658
cert-bund: WID-SEC-2023-0431
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354

[[return to 192.168.220.129](#)]

2.1.20 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

Summary

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

Quality of Detection (QoD): 80%

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

It was detected that the host implements RFC1323/RFC7323.

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

Packet 1: 789014

Packet 2: 789121

Impact

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

Solution:

Solution type: Mitigation

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

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

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

See the references for more information.

Affected Software/OS

TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight

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

Vulnerability Detection Method

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

Details: TCP Timestamps Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.80091

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

References

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

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

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

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

[[return to 192.168.220.129](#)]

2.1.21 Low general/icmp

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

[[return to 192.168.220.129](#)]

2.1.22 Low 5432/tcp

Low (CVSS: 3.4) NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)
Product detection result cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.→802067)
Summary This host is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.
Solution: Solution type: Mitigation Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+
Vulnerability Insight The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code
Vulnerability Detection Method Evaluate previous collected information about this service. Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability . →.. OID:1.3.6.1.4.1.25623.1.0.802087 Version used: 2024-09-30T08:38:05Z
Product Detection Result Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Report Supported Cipher Suites ... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.802067)

References

cve: CVE-2014-3566
url: <https://www.openssl.org/~bodo/ssl-poodle.pdf>
url: <http://www.securityfocus.com/bid/70574>
url: <https://www.imperialviolet.org/2014/10/14/poodle.html>
url: <https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html>
url: <http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin.html>
cert-bund: WID-SEC-2025-1658
cert-bund: WID-SEC-2023-0431
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342

... continues on next page ...

... continued from previous page ...

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

[[return to 192.168.220.129](#)]