

# Scan Report

March 28, 2024

## Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Immediate scan of IP hr.ep.int.e-netsec.org”. The scan started at Thu Mar 28 22:27:57 2024 UTC and ended at Thu Mar 28 23:14:34 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

<b>1</b>	<b>Result Overview</b>	<b>2</b>
<b>2</b>	<b>Results per Host</b>	<b>2</b>
2.1	10.10.152.150 . . . . .	2
2.1.1	High general/tcp . . . . .	2
2.1.2	High 443/tcp . . . . .	4
2.1.3	Medium 80/tcp . . . . .	8
2.1.4	Medium 443/tcp . . . . .	12
2.1.5	Medium 2222/tcp . . . . .	26
2.1.6	Low general/icmp . . . . .	30
2.1.7	Low general/tcp . . . . .	31
2.1.8	Low 443/tcp . . . . .	32
2.1.9	Low 2222/tcp . . . . .	35

## 1 Result Overview

Host	High	Medium	Low	Log	False Positive
<a href="#">10.10.152.150</a> <a href="#">hr.ep.int.e-netsec.org</a>	3	14	4	0	0
Total: 1	3	14	4	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 21 results selected by the filtering described above. Before filtering there were 442 results.

## 2 Results per Host

### 2.1 10.10.152.150

Host scan start Thu Mar 28 22:29:25 2024 UTC

Host scan end Thu Mar 28 23:14:16 2024 UTC

Service (Port)	Threat Level
<a href="#">general/tcp</a>	High
<a href="#">443/tcp</a>	High
<a href="#">80/tcp</a>	Medium
<a href="#">443/tcp</a>	Medium
<a href="#">2222/tcp</a>	Medium
<a href="#">general/icmp</a>	Low
<a href="#">general/tcp</a>	Low
<a href="#">443/tcp</a>	Low
<a href="#">2222/tcp</a>	Low

#### 2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: Operating System (OS) End of Life (EOL) Detection
<p><b>Product detection result</b></p> <p>cpe:/o:debian:debian_linux:7</p> <p>Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0 ↪.105937)</p>
<p><b>Summary</b></p> <p>The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.</p>
<p><b>Quality of Detection:</b> 80</p>
<p><b>Vulnerability Detection Result</b></p> <p>The "Debian GNU/Linux" Operating System on the remote host has reached the end of life.</p> <p>CPE: cpe:/o:debian:debian_linux:7</p> <p>Installed version, build or SP: 7</p> <p>EOL date: 2018-05-31</p> <p>EOL info: <a href="https://en.wikipedia.org/wiki/List_of_Debian_releases#Release_table">https://en.wikipedia.org/wiki/List_of_Debian_releases#Release ↪_table</a></p>
<p><b>Impact</b></p> <p>An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Checks if an EOL version of an OS is present on the target host.</p> <p>Details: Operating System (OS) End of Life (EOL) Detection</p> <p>OID:1.3.6.1.4.1.25623.1.0.103674</p> <p>Version used: 2024-02-28T14:37:42Z</p>
<p><b>Product Detection Result</b></p> <p>Product: cpe:/o:debian:debian_linux:7</p> <p>Method: OS Detection Consolidation and Reporting</p> <p>OID: 1.3.6.1.4.1.25623.1.0.105937)</p>

## 2.1.2 High 443/tcp

High (CVSS: 7.5)
NVT: SSL/TLS: OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability
<b>Summary</b> OpenSSL is prone to an information disclosure vulnerability.
<b>Quality of Detection:</b> 99
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> An attacker can exploit this issue to gain access to sensitive information that may aid in further attacks.
<b>Solution:</b> <b>Solution type:</b> VendorFix Updates are available. Please see the references for more information.
<b>Affected Software/OS</b> OpenSSL 1.0.1f, 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, and 1.0.1 are vulnerable.
<b>Vulnerability Insight</b> The TLS and DTLS implementations do not properly handle Heartbeat Extension packets.
<b>Vulnerability Detection Method</b> Send a special crafted TLS request and check the response. Details: SSL/TLS: OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability OID:1.3.6.1.4.1.25623.1.0.103936 Version used: 2023-04-18T10:19:20Z
<b>References</b> cve: CVE-2014-0160 cisa: Known Exploited Vulnerability (KEV) catalog url: <a href="https://www.cisa.gov/known-exploited-vulnerabilities-catalog">https://www.cisa.gov/known-exploited-vulnerabilities-catalog</a> url: <a href="https://www.openssl.org/news/secadv/20140407.txt">https://www.openssl.org/news/secadv/20140407.txt</a> url: <a href="http://www.securityfocus.com/bid/66690">http://www.securityfocus.com/bid/66690</a> cert-bund: CB-K16/0719 cert-bund: CB-K14/0482 cert-bund: CB-K14/0458 cert-bund: CB-K14/0406 cert-bund: CB-K14/0405 dfn-cert: DFN-CERT-2016-0773
... continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2014-0495
dfn-cert: DFN-CERT-2014-0483
dfn-cert: DFN-CERT-2014-0421
dfn-cert: DFN-CERT-2014-0420
```

High (CVSS: 7.5)

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

**Summary**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Solution:**

**Solution type:** Mitigation

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

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

**Affected Software/OS**

Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

**Vulnerability Insight**

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

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

**Vulnerability Detection Method**

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

OID:1.3.6.1.4.1.25623.1.0.108031

... continues on next page ...

...continued from previous page ...

Version used: 2023-07-20T05:05:17Z

**References**

cve: CVE-2016-2183  
 cve: CVE-2016-6329  
 cve: CVE-2020-12872  
 url: <https://bettercrypto.org/>  
 url: <https://mozilla.github.io/server-side-tls/ssl-config-generator/>  
 url: <https://sweet32.info/>  
 cert-bund: WID-SEC-2024-0209  
 cert-bund: WID-SEC-2024-0064  
 cert-bund: WID-SEC-2022-2226  
 cert-bund: WID-SEC-2022-1955  
 cert-bund: CB-K21/1094  
 cert-bund: CB-K20/1023  
 cert-bund: CB-K20/0321  
 cert-bund: CB-K20/0314  
 cert-bund: CB-K20/0157  
 cert-bund: CB-K19/0618  
 cert-bund: CB-K19/0615  
 cert-bund: CB-K18/0296  
 cert-bund: CB-K17/1980  
 cert-bund: CB-K17/1871  
 cert-bund: CB-K17/1803  
 cert-bund: CB-K17/1753  
 cert-bund: CB-K17/1750  
 cert-bund: CB-K17/1709  
 cert-bund: CB-K17/1558  
 cert-bund: CB-K17/1273  
 cert-bund: CB-K17/1202  
 cert-bund: CB-K17/1196  
 cert-bund: CB-K17/1055  
 cert-bund: CB-K17/1026  
 cert-bund: CB-K17/0939  
 cert-bund: CB-K17/0917  
 cert-bund: CB-K17/0915  
 cert-bund: CB-K17/0877  
 cert-bund: CB-K17/0796  
 cert-bund: CB-K17/0724  
 cert-bund: CB-K17/0661  
 cert-bund: CB-K17/0657  
 cert-bund: CB-K17/0582  
 cert-bund: CB-K17/0581  
 cert-bund: CB-K17/0506  
 cert-bund: CB-K17/0504  
 cert-bund: CB-K17/0467  
 cert-bund: CB-K17/0345

...continues on next page ...

...continued from previous page ...

cert-bund: CB-K17/0098  
cert-bund: CB-K17/0089  
cert-bund: CB-K17/0086  
cert-bund: CB-K17/0082  
cert-bund: CB-K16/1837  
cert-bund: CB-K16/1830  
cert-bund: CB-K16/1635  
cert-bund: CB-K16/1630  
cert-bund: CB-K16/1624  
cert-bund: CB-K16/1622  
cert-bund: CB-K16/1500  
cert-bund: CB-K16/1465  
cert-bund: CB-K16/1307  
cert-bund: CB-K16/1296  
dfn-cert: DFN-CERT-2021-1618  
dfn-cert: DFN-CERT-2021-0775  
dfn-cert: DFN-CERT-2021-0770  
dfn-cert: DFN-CERT-2021-0274  
dfn-cert: DFN-CERT-2020-2141  
dfn-cert: DFN-CERT-2020-0368  
dfn-cert: DFN-CERT-2019-1455  
dfn-cert: DFN-CERT-2019-0068  
dfn-cert: DFN-CERT-2018-1296  
dfn-cert: DFN-CERT-2018-0323  
dfn-cert: DFN-CERT-2017-2070  
dfn-cert: DFN-CERT-2017-1954  
dfn-cert: DFN-CERT-2017-1885  
dfn-cert: DFN-CERT-2017-1831  
dfn-cert: DFN-CERT-2017-1821  
dfn-cert: DFN-CERT-2017-1785  
dfn-cert: DFN-CERT-2017-1626  
dfn-cert: DFN-CERT-2017-1326  
dfn-cert: DFN-CERT-2017-1239  
dfn-cert: DFN-CERT-2017-1238  
dfn-cert: DFN-CERT-2017-1090  
dfn-cert: DFN-CERT-2017-1060  
dfn-cert: DFN-CERT-2017-0968  
dfn-cert: DFN-CERT-2017-0947  
dfn-cert: DFN-CERT-2017-0946  
dfn-cert: DFN-CERT-2017-0904  
dfn-cert: DFN-CERT-2017-0816  
dfn-cert: DFN-CERT-2017-0746  
dfn-cert: DFN-CERT-2017-0677  
dfn-cert: DFN-CERT-2017-0675  
dfn-cert: DFN-CERT-2017-0611  
dfn-cert: DFN-CERT-2017-0609  
dfn-cert: DFN-CERT-2017-0522

...continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[\[ return to 10.10.152.150 \]](#)**2.1.3 Medium 80/tcp**

Medium (CVSS: 6.1)

NVT: jQuery &lt; 1.9.0 XSS Vulnerability

**Summary**

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

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

Installed version: 1.4.4

Fixed version: 1.9.0

Installation

path / port: /phpmyadmin/js/jquery/jquery-1.4.4.js

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

- Identified file: <http://hr.ep.int.e-netsec.org/phpmyadmin/js/jquery/jquery-1.4.4.js>

- Referenced at: <http://hr.ep.int.e-netsec.org/phpmyadmin/>

**Solution:****Solution type:** VendorFix

Update to version 1.9.0 or later.

... continues on next page ...



...continued from previous page ...
<b>Affected Software/OS</b> jQuery prior to version 1.9.0.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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 Version used: 2023-07-14T05:06:08Z
<b>References</b> cve: CVE-2012-6708 url: <a href="https://bugs.jquery.com/ticket/11290">https://bugs.jquery.com/ticket/11290</a> cert-bund: WID-SEC-2022-0673 cert-bund: CB-K22/0045 cert-bund: CB-K18/1131 dfn-cert: DFN-CERT-2023-1197 dfn-cert: DFN-CERT-2020-0590

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP
<b>Summary</b> The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.
<b>Quality of Detection: 80</b>
<b>Vulnerability Detection Result</b> The following URLs requires Basic Authentication (URL:realm name): <a href="http://hr.ep.int.e-netsec.org/phpmyadmin/setup/">http://hr.ep.int.e-netsec.org/phpmyadmin/setup/</a> : "phpMyAdmin Setup"
<b>Impact</b> 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.
... continues on next page ...

...continued from previous page ...
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.
<b>Vulnerability Detection Method</b> Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection. The script is currently checking the following: - HTTP Basic Authentication (Basic Auth) - HTTP Forms (e.g. Login) with input field of type 'password' Details: Cleartext Transmission of Sensitive Information via HTTP OID:1.3.6.1.4.1.25623.1.0.108440 Version used: 2023-09-07T05:05:21Z
<b>References</b> url: <a href="https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management">https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management</a> url: <a href="https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure">https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure</a> url: <a href="https://cwe.mitre.org/data/definitions/319.html">https://cwe.mitre.org/data/definitions/319.html</a>

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability
<b>Summary</b> jQuery is prone to a cross-site scripting (XSS) vulnerability.
<b>Quality of Detection:</b> 80
<b>Vulnerability Detection Result</b> Installed version: 1.4.4 Fixed version: 1.6.3 Installation path / port: /phpmyadmin/js/jquery/jquery-1.4.4.js Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info): - Identified file: <a href="http://hr.ep.int.e-netsec.org/phpmyadmin/js/jquery/jquery-1.4.4.js">http://hr.ep.int.e-netsec.org/phpmyadmin/js/jquery/jquery-1.4.4.js</a> - Referenced at: <a href="http://hr.ep.int.e-netsec.org/phpmyadmin/">http://hr.ep.int.e-netsec.org/phpmyadmin/</a>
... continues on next page ...

...continued from previous page ...
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 1.6.3 or later.
<b>Affected Software/OS</b> jQuery prior to version 1.6.3.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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
<b>References</b> cve: CVE-2011-4969 url: <a href="https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/">https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/</a> cert-bund: CB-K17/0195 dfn-cert: DFN-CERT-2017-0199 dfn-cert: DFN-CERT-2016-0890

Medium (CVSS: 4.3)
NVT: Apache HTTP Server ETag Header Information Disclosure Weakness
<b>Product detection result</b> cpe:/a:apache:http_server:2.2.22 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1 ↪.0.117232)
<b>Summary</b> A weakness has been discovered in the Apache HTTP Server if configured to use the FileETag directive.
<b>Quality of Detection:</b> 80
<b>Vulnerability Detection Result</b> Information that was gathered: Inode: 148677 Size: 230
... continues on next page ...

...continued from previous page...	
<b>Impact</b>	Exploitation of this issue may provide an attacker with information that may be used to launch further attacks against a target network.
<b>Solution:</b>	<p><b>Solution type:</b> VendorFix</p> <p>OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information.</p> <p>Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare. Please see the attached Technical Information Document for further details.</p>
<b>Vulnerability Detection Method</b>	<p>Due to the way in which Apache HTTP Server generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields returned to a client contain the file's inode number.</p> <p>Details: Apache HTTP Server ETag Header Information Disclosure Weakness</p> <p>OID:1.3.6.1.4.1.25623.1.0.103122</p> <p>Version used: 2022-12-05T10:11:03Z</p>
<b>Product Detection Result</b>	<p>Product: cpe:/a:apache:http_server:2.2.22</p> <p>Method: Apache HTTP Server Detection Consolidation</p> <p>OID: 1.3.6.1.4.1.25623.1.0.117232)</p>
<b>References</b>	<p>cve: CVE-2003-1418</p> <p>url: <a href="http://www.securityfocus.com/bid/6939">http://www.securityfocus.com/bid/6939</a></p> <p>url: <a href="http://httpd.apache.org/docs/mod/core.html#fileetag">http://httpd.apache.org/docs/mod/core.html#fileetag</a></p> <p>url: <a href="http://www.openbsd.org/errata32.html">http://www.openbsd.org/errata32.html</a></p> <p>url: <a href="http://support.novell.com/docs/Tids/Solutions/10090670.html">http://support.novell.com/docs/Tids/Solutions/10090670.html</a></p> <p>cert-bund: CB-K17/1750</p> <p>cert-bund: CB-K17/0896</p> <p>cert-bund: CB-K15/0469</p> <p>dfn-cert: DFN-CERT-2017-1821</p> <p>dfn-cert: DFN-CERT-2017-0925</p> <p>dfn-cert: DFN-CERT-2015-0495</p>

[\[ return to 10.10.152.150 \]](#)

### 2.1.4 Medium 443/tcp

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability
<b>Summary</b> jQuery is prone to a cross-site scripting (XSS) vulnerability.
<b>Quality of Detection: 80</b>
<b>Vulnerability Detection Result</b> Installed version: 1.4.4 Fixed version: 1.9.0 Installation path / port: /phpmyadmin/js/jquery/jquery-1.4.4.js Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info): - Identified file: <a href="https://hr.ep.int.e-netsec.org/phpmyadmin/js/jquery/jquery-1.4.4.js">https://hr.ep.int.e-netsec.org/phpmyadmin/js/jquery/jquery-1.4.4.js</a> - Referenced at: <a href="https://hr.ep.int.e-netsec.org/phpmyadmin/">https://hr.ep.int.e-netsec.org/phpmyadmin/</a>
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 1.9.0 or later.
<b>Affected Software/OS</b> jQuery prior to version 1.9.0.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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 Version used: 2023-07-14T05:06:08Z
<b>References</b> cve: CVE-2012-6708 url: <a href="https://bugs.jquery.com/ticket/11290">https://bugs.jquery.com/ticket/11290</a> cert-bund: WID-SEC-2022-0673 cert-bund: CB-K22/0045 cert-bund: CB-K18/1131
... continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2023-1197  
 dfn-cert: DFN-CERT-2020-0590

Medium (CVSS: 5.9)

NVT: SSL/TLS: Report Weak Cipher Suites

**Summary**

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

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

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

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

TLS\_RSA\_WITH\_RC4\_128\_SHA

TLS\_RSA\_WITH\_SEED\_CBC\_SHA

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

TLS\_RSA\_WITH\_RC4\_128\_SHA

TLS\_RSA\_WITH\_SEED\_CBC\_SHA

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

TLS\_RSA\_WITH\_RC4\_128\_SHA

TLS\_RSA\_WITH\_SEED\_CBC\_SHA

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

TLS\_RSA\_WITH\_RC4\_128\_SHA

TLS\_RSA\_WITH\_SEED\_CBC\_SHA

**Solution:**

**Solution type:** Mitigation

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

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

**Vulnerability Insight**

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

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

**Vulnerability Detection Method**

... continues on next page ...

...continued from previous page ...

Details: SSL/TLS: Report Weak Cipher Suites  
 OID:1.3.6.1.4.1.25623.1.0.103440  
 Version used: 2023-11-02T05:05:26Z

**References**

cve: CVE-2013-2566  
 cve: CVE-2015-2808  
 cve: CVE-2015-4000  
 url: [https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung\\_cb-k16-1↪465\\_update\\_6.html](https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1↪465_update_6.html)  
 url: <https://bettercrypto.org/>  
 url: <https://mozilla.github.io/server-side-tls/ssl-config-generator/>  
 cert-bund: CB-K21/0067  
 cert-bund: CB-K19/0812  
 cert-bund: CB-K17/1750  
 cert-bund: CB-K16/1593  
 cert-bund: CB-K16/1552  
 cert-bund: CB-K16/1102  
 cert-bund: CB-K16/0617  
 cert-bund: CB-K16/0599  
 cert-bund: CB-K16/0168  
 cert-bund: CB-K16/0121  
 cert-bund: CB-K16/0090  
 cert-bund: CB-K16/0030  
 cert-bund: CB-K15/1751  
 cert-bund: CB-K15/1591  
 cert-bund: CB-K15/1550  
 cert-bund: CB-K15/1517  
 cert-bund: CB-K15/1514  
 cert-bund: CB-K15/1464  
 cert-bund: CB-K15/1442  
 cert-bund: CB-K15/1334  
 cert-bund: CB-K15/1269  
 cert-bund: CB-K15/1136  
 cert-bund: CB-K15/1090  
 cert-bund: CB-K15/1059  
 cert-bund: CB-K15/1022  
 cert-bund: CB-K15/1015  
 cert-bund: CB-K15/0986  
 cert-bund: CB-K15/0964  
 cert-bund: CB-K15/0962  
 cert-bund: CB-K15/0932  
 cert-bund: CB-K15/0927  
 cert-bund: CB-K15/0926  
 cert-bund: CB-K15/0907  
 cert-bund: CB-K15/0901  
 cert-bund: CB-K15/0896

...continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0889  
cert-bund: CB-K15/0877  
cert-bund: CB-K15/0850  
cert-bund: CB-K15/0849  
cert-bund: CB-K15/0834  
cert-bund: CB-K15/0827  
cert-bund: CB-K15/0802  
cert-bund: CB-K15/0764  
cert-bund: CB-K15/0733  
cert-bund: CB-K15/0667  
cert-bund: CB-K14/0935  
cert-bund: CB-K13/0942  
dfn-cert: DFN-CERT-2023-2939  
dfn-cert: DFN-CERT-2021-0775  
dfn-cert: DFN-CERT-2020-1561  
dfn-cert: DFN-CERT-2020-1276  
dfn-cert: DFN-CERT-2017-1821  
dfn-cert: DFN-CERT-2016-1692  
dfn-cert: DFN-CERT-2016-1648  
dfn-cert: DFN-CERT-2016-1168  
dfn-cert: DFN-CERT-2016-0665  
dfn-cert: DFN-CERT-2016-0642  
dfn-cert: DFN-CERT-2016-0184  
dfn-cert: DFN-CERT-2016-0135  
dfn-cert: DFN-CERT-2016-0101  
dfn-cert: DFN-CERT-2016-0035  
dfn-cert: DFN-CERT-2015-1853  
dfn-cert: DFN-CERT-2015-1679  
dfn-cert: DFN-CERT-2015-1632  
dfn-cert: DFN-CERT-2015-1608  
dfn-cert: DFN-CERT-2015-1542  
dfn-cert: DFN-CERT-2015-1518  
dfn-cert: DFN-CERT-2015-1406  
dfn-cert: DFN-CERT-2015-1341  
dfn-cert: DFN-CERT-2015-1194  
dfn-cert: DFN-CERT-2015-1144  
dfn-cert: DFN-CERT-2015-1113  
dfn-cert: DFN-CERT-2015-1078  
dfn-cert: DFN-CERT-2015-1067  
dfn-cert: DFN-CERT-2015-1038  
dfn-cert: DFN-CERT-2015-1016  
dfn-cert: DFN-CERT-2015-1012  
dfn-cert: DFN-CERT-2015-0980  
dfn-cert: DFN-CERT-2015-0977  
dfn-cert: DFN-CERT-2015-0976  
dfn-cert: DFN-CERT-2015-0960  
dfn-cert: DFN-CERT-2015-0956

...continues on next page ...



...continued from previous page ...

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

Medium (CVSS: 5.9)

NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Summary**

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

**Quality of Detection:** 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) VT.

**Impact**

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

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

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

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

**Affected Software/OS**

All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**

... continues on next page ...

...continued from previous page ...
<p>The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:</p> <ul style="list-style-type: none"> <li>- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)</li> <li>- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)</li> </ul>
<p><b>Vulnerability Detection Method</b></p> <p>Check the used SSL protocols of the services provided by this system.  Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection  OID:1.3.6.1.4.1.25623.1.0.111012  Version used: 2021-10-15T12:51:02Z</p>
<p><b>References</b></p> <p>cve: CVE-2016-0800  cve: CVE-2014-3566  url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a>  url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a>  url: <a href="https://drownattack.com/">https://drownattack.com/</a>  url: <a href="https://www.imperialviolet.org/2014/10/14/poodle.html">https://www.imperialviolet.org/2014/10/14/poodle.html</a>  url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a>  ↔-report-2014  cert-bund: WID-SEC-2023-0431  cert-bund: WID-SEC-2023-0427  cert-bund: CB-K18/0094  cert-bund: CB-K17/1198  cert-bund: CB-K17/1196  cert-bund: CB-K16/1828  cert-bund: CB-K16/1438  cert-bund: CB-K16/1384  cert-bund: CB-K16/1141  cert-bund: CB-K16/1107  cert-bund: CB-K16/1102  cert-bund: CB-K16/0792  cert-bund: CB-K16/0599  cert-bund: CB-K16/0597  cert-bund: CB-K16/0459  cert-bund: CB-K16/0456  cert-bund: CB-K16/0433  cert-bund: CB-K16/0424  cert-bund: CB-K16/0415  cert-bund: CB-K16/0413  cert-bund: CB-K16/0374  cert-bund: CB-K16/0367  cert-bund: CB-K16/0331  cert-bund: CB-K16/0329  cert-bund: CB-K16/0328  cert-bund: CB-K16/0156  cert-bund: CB-K15/1514  cert-bund: CB-K15/1358</p>
...continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/1021  
cert-bund: CB-K15/0972  
cert-bund: CB-K15/0637  
cert-bund: CB-K15/0590  
cert-bund: CB-K15/0525  
cert-bund: CB-K15/0393  
cert-bund: CB-K15/0384  
cert-bund: CB-K15/0287  
cert-bund: CB-K15/0252  
cert-bund: CB-K15/0246  
cert-bund: CB-K15/0237  
cert-bund: CB-K15/0118  
cert-bund: CB-K15/0110  
cert-bund: CB-K15/0108  
cert-bund: CB-K15/0080  
cert-bund: CB-K15/0078  
cert-bund: CB-K15/0077  
cert-bund: CB-K15/0075  
cert-bund: CB-K14/1617  
cert-bund: CB-K14/1581  
cert-bund: CB-K14/1537  
cert-bund: CB-K14/1479  
cert-bund: CB-K14/1458  
cert-bund: CB-K14/1342  
cert-bund: CB-K14/1314  
cert-bund: CB-K14/1313  
cert-bund: CB-K14/1311  
cert-bund: CB-K14/1304  
cert-bund: CB-K14/1296  
dfn-cert: DFN-CERT-2018-0096  
dfn-cert: DFN-CERT-2017-1238  
dfn-cert: DFN-CERT-2017-1236  
dfn-cert: DFN-CERT-2016-1929  
dfn-cert: DFN-CERT-2016-1527  
dfn-cert: DFN-CERT-2016-1468  
dfn-cert: DFN-CERT-2016-1216  
dfn-cert: DFN-CERT-2016-1174  
dfn-cert: DFN-CERT-2016-1168  
dfn-cert: DFN-CERT-2016-0884  
dfn-cert: DFN-CERT-2016-0841  
dfn-cert: DFN-CERT-2016-0644  
dfn-cert: DFN-CERT-2016-0642  
dfn-cert: DFN-CERT-2016-0496  
dfn-cert: DFN-CERT-2016-0495  
dfn-cert: DFN-CERT-2016-0465  
dfn-cert: DFN-CERT-2016-0459  
dfn-cert: DFN-CERT-2016-0453

...continues on next page ...

...continued from previous page ...

```

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: 4.3)

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

**Summary**

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

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

In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and ↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c  
... continues on next page ...

...continued from previous page ...
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
<p><b>Impact</b></p> <p>An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.</p> <p>Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.</p>
<p><b>Solution:</b></p> <p><b>Solution type:</b> Mitigation</p> <p>It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.</p>
<p><b>Affected Software/OS</b></p> <p>All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.</p>
<p><b>Vulnerability Insight</b></p> <p>The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:</p> <ul style="list-style-type: none"> <li>- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)</li> <li>- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)</li> </ul>
<p><b>Vulnerability Detection Method</b></p> <p>Check the used TLS protocols of the services provided by this system.</p> <p>Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection</p> <p>OID:1.3.6.1.4.1.25623.1.0.117274</p> <p>Version used: 2023-10-20T16:09:12Z</p>
<p><b>References</b></p> <p>cve: CVE-2011-3389</p> <p>cve: CVE-2015-0204</p> <p>url: <a href="https://ssl-config.mozilla.org/">https://ssl-config.mozilla.org/</a></p> <p>url: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a></p> <p>url: <a href="https://datatracker.ietf.org/doc/rfc8996/">https://datatracker.ietf.org/doc/rfc8996/</a></p> <p>url: <a href="https://vnhacker.blogspot.com/2011/09/beast.html">https://vnhacker.blogspot.com/2011/09/beast.html</a></p> <p>url: <a href="https://web.archive.org/web/20201108095603/https://censys.io/blog/freak">https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</a></p> <p>url: <a href="https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters">https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</a></p> <p>↪-report-2014</p> <p>cert-bund: WID-SEC-2023-1435</p> <p>cert-bund: CB-K18/0799</p> <p>cert-bund: CB-K16/1289</p> <p>cert-bund: CB-K16/1096</p> <p>cert-bund: CB-K15/1751</p> <p>cert-bund: CB-K15/1266</p>
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/0850  
 cert-bund: CB-K15/0764  
 cert-bund: CB-K15/0720  
 cert-bund: CB-K15/0548  
 cert-bund: CB-K15/0526  
 cert-bund: CB-K15/0509  
 cert-bund: CB-K15/0493  
 cert-bund: CB-K15/0384  
 cert-bund: CB-K15/0365  
 cert-bund: CB-K15/0364  
 cert-bund: CB-K15/0302  
 cert-bund: CB-K15/0192  
 cert-bund: CB-K15/0079  
 cert-bund: CB-K15/0016  
 cert-bund: CB-K14/1342  
 cert-bund: CB-K14/0231  
 cert-bund: CB-K13/0845  
 cert-bund: CB-K13/0796  
 cert-bund: CB-K13/0790  
 dfn-cert: DFN-CERT-2020-0177  
 dfn-cert: DFN-CERT-2020-0111  
 dfn-cert: DFN-CERT-2019-0068  
 dfn-cert: DFN-CERT-2018-1441  
 dfn-cert: DFN-CERT-2018-1408  
 dfn-cert: DFN-CERT-2016-1372  
 dfn-cert: DFN-CERT-2016-1164  
 dfn-cert: DFN-CERT-2016-0388  
 dfn-cert: DFN-CERT-2015-1853  
 dfn-cert: DFN-CERT-2015-1332  
 dfn-cert: DFN-CERT-2015-0884  
 dfn-cert: DFN-CERT-2015-0800  
 dfn-cert: DFN-CERT-2015-0758  
 dfn-cert: DFN-CERT-2015-0567  
 dfn-cert: DFN-CERT-2015-0544  
 dfn-cert: DFN-CERT-2015-0530  
 dfn-cert: DFN-CERT-2015-0396  
 dfn-cert: DFN-CERT-2015-0375  
 dfn-cert: DFN-CERT-2015-0374  
 dfn-cert: DFN-CERT-2015-0305  
 dfn-cert: DFN-CERT-2015-0199  
 dfn-cert: DFN-CERT-2015-0079  
 dfn-cert: DFN-CERT-2015-0021  
 dfn-cert: DFN-CERT-2014-1414  
 dfn-cert: DFN-CERT-2013-1847  
 dfn-cert: DFN-CERT-2013-1792  
 dfn-cert: DFN-CERT-2012-1979  
 dfn-cert: DFN-CERT-2012-1829

...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2012-1530  
dfn-cert: DFN-CERT-2012-1380  
dfn-cert: DFN-CERT-2012-1377  
dfn-cert: DFN-CERT-2012-1292  
dfn-cert: DFN-CERT-2012-1214  
dfn-cert: DFN-CERT-2012-1213  
dfn-cert: DFN-CERT-2012-1180  
dfn-cert: DFN-CERT-2012-1156  
dfn-cert: DFN-CERT-2012-1155  
dfn-cert: DFN-CERT-2012-1039  
dfn-cert: DFN-CERT-2012-0956  
dfn-cert: DFN-CERT-2012-0908  
dfn-cert: DFN-CERT-2012-0868  
dfn-cert: DFN-CERT-2012-0867  
dfn-cert: DFN-CERT-2012-0848  
dfn-cert: DFN-CERT-2012-0838  
dfn-cert: DFN-CERT-2012-0776  
dfn-cert: DFN-CERT-2012-0722  
dfn-cert: DFN-CERT-2012-0638  
dfn-cert: DFN-CERT-2012-0627  
dfn-cert: DFN-CERT-2012-0451  
dfn-cert: DFN-CERT-2012-0418  
dfn-cert: DFN-CERT-2012-0354  
dfn-cert: DFN-CERT-2012-0234  
dfn-cert: DFN-CERT-2012-0221  
dfn-cert: DFN-CERT-2012-0177  
dfn-cert: DFN-CERT-2012-0170  
dfn-cert: DFN-CERT-2012-0146  
dfn-cert: DFN-CERT-2012-0142  
dfn-cert: DFN-CERT-2012-0126  
dfn-cert: DFN-CERT-2012-0123  
dfn-cert: DFN-CERT-2012-0095  
dfn-cert: DFN-CERT-2012-0051  
dfn-cert: DFN-CERT-2012-0047  
dfn-cert: DFN-CERT-2012-0021  
dfn-cert: DFN-CERT-2011-1953  
dfn-cert: DFN-CERT-2011-1946  
dfn-cert: DFN-CERT-2011-1844  
dfn-cert: DFN-CERT-2011-1826  
dfn-cert: DFN-CERT-2011-1774  
dfn-cert: DFN-CERT-2011-1743  
dfn-cert: DFN-CERT-2011-1738  
dfn-cert: DFN-CERT-2011-1706  
dfn-cert: DFN-CERT-2011-1628  
dfn-cert: DFN-CERT-2011-1627  
dfn-cert: DFN-CERT-2011-1619  
dfn-cert: DFN-CERT-2011-1482

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability
<b>Summary</b> jQuery is prone to a cross-site scripting (XSS) vulnerability.
<b>Quality of Detection:</b> 80
<b>Vulnerability Detection Result</b> Installed version: 1.4.4 Fixed version: 1.6.3 Installation path / port: /phpmyadmin/js/jquery/jquery-1.4.4.js Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info): - Identified file: <a href="https://hr.ep.int.e-netsec.org/phpmyadmin/js/jquery/jquery-1.4.4.js">https://hr.ep.int.e-netsec.org/phpmyadmin/js/jquery/jquery-1.4.4.js</a> - Referenced at: <a href="https://hr.ep.int.e-netsec.org/phpmyadmin/">https://hr.ep.int.e-netsec.org/phpmyadmin/</a>
<b>Solution:</b> <b>Solution type:</b> VendorFix Update to version 1.6.3 or later.
<b>Affected Software/OS</b> jQuery prior to version 1.6.3.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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
<b>References</b> cve: CVE-2011-4969 url: <a href="https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/">https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/</a> cert-bund: CB-K17/0195 dfn-cert: DFN-CERT-2017-0199 dfn-cert: DFN-CERT-2016-0890



Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
<b>Summary</b> The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.
<b>Quality of Detection:</b> 80
<b>Vulnerability Detection Result</b> The following certificates are part of the certificate chain but using insecure ↪signature algorithms: Subject: CN=hr Signature Algorithm: sha1WithRSAEncryption
<b>Solution:</b> <b>Solution type:</b> Mitigation Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.
<b>Vulnerability Insight</b> The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use: <ul style="list-style-type: none"> <li>- Secure Hash Algorithm 1 (SHA-1)</li> <li>- Message Digest 5 (MD5)</li> <li>- Message Digest 4 (MD4)</li> <li>- Message Digest 2 (MD2)</li> </ul> Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates. NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive: Fingerprint1 or fingerprint1, Fingerprint2
<b>Vulnerability Detection Method</b> Check which hashing algorithm was used to sign the remote SSL/TLS certificate. Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm OID:1.3.6.1.4.1.25623.1.0.105880 Version used: 2021-10-15T11:13:32Z
<b>References</b> ... continues on next page ...

...continued from previous page...	
url: <a href="https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/">https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/</a>	
Medium (CVSS: 4.0)	
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	
<b>Summary</b> The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).	
<b>Quality of Detection:</b> 80	
<b>Vulnerability Detection Result</b> Server Temporary Key Size: 1024 bits	
<b>Impact</b> An attacker might be able to decrypt the SSL/TLS communication offline.	
<b>Solution:</b> <b>Solution type:</b> Workaround Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.	
<b>Vulnerability Insight</b> 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.	
<b>Vulnerability Detection Method</b> Checks the DHE temporary public key size. Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability. ↪.. OID:1.3.6.1.4.1.25623.1.0.106223 Version used: 2023-07-21T05:05:22Z	
<b>References</b> url: <a href="https://weakdh.org/">https://weakdh.org/</a> url: <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a>	

[ [return to 10.10.152.150](#) ]

### 2.1.5 Medium 2222/tcp

Medium (CVSS: 5.3)
NVT: Weak Host Key Algorithm(s) (SSH)
<b>Summary</b> The remote SSH server is configured to allow / support weak host key algorithm(s).
<b>Quality of Detection: 80</b>
<b>Vulnerability Detection Result</b> The remote SSH server supports the following weak host key algorithm(s): host key algorithm   Description ----- ↪----- ssh-dss   Digital Signature Algorithm (DSA) / Digital Signature Stand ↪ard (DSS)
<b>Solution:</b> <b>Solution type:</b> Mitigation Disable the reported weak host key algorithm(s).
<b>Vulnerability Detection Method</b> Checks the supported host key algorithms of the remote SSH server. Currently weak host key algorithms are defined as the following: - ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS) Details: Weak Host Key Algorithm(s) (SSH) OID:1.3.6.1.4.1.25623.1.0.117687 Version used: 2023-10-12T05:05:32Z
<b>References</b> url: <a href="https://www.rfc-editor.org/rfc/rfc8332">https://www.rfc-editor.org/rfc/rfc8332</a> url: <a href="https://www.rfc-editor.org/rfc/rfc8709">https://www.rfc-editor.org/rfc/rfc8709</a> url: <a href="https://www.rfc-editor.org/rfc/rfc4253#section-6.6">https://www.rfc-editor.org/rfc/rfc4253#section-6.6</a>

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)
<b>Summary</b> The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).
<b>Quality of Detection: 80</b>
<b>Vulnerability Detection Result</b> The remote SSH server supports the following weak KEX algorithm(s): ... continues on next page ...

...continued from previous page...	
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	
<b>Impact</b> An attacker can quickly break individual connections.	
<b>Solution:</b> <b>Solution type:</b> 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.	
<b>Vulnerability Insight</b> - 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.	
<b>Vulnerability Detection Method</b> Checks the supported KEX algorithms of the remote SSH server. Currently weak KEX algorithms are defined as the following: - non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime - ephemerally generated key exchange groups uses SHA-1 - using RSA 1024-bit modulus key Details: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.150713 Version used: 2023-10-12T05:05:32Z	
<b>References</b> url: <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a> url: <a href="https://www.rfc-editor.org/rfc/rfc9142">https://www.rfc-editor.org/rfc/rfc9142</a> url: <a href="https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implementations">https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implementations</a> url: <a href="https://www.rfc-editor.org/rfc/rfc6194">https://www.rfc-editor.org/rfc/rfc6194</a> url: <a href="https://www.rfc-editor.org/rfc/rfc4253#section-6.5">https://www.rfc-editor.org/rfc/rfc4253#section-6.5</a>	

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)
<b>Summary</b> The remote SSH server is configured to allow / support weak encryption algorithm(s).
<b>Quality of Detection: 80</b>
<b>Vulnerability Detection Result</b> The remote SSH server supports the following weak client-to-server encryption al gorithm(s): 3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se The remote SSH server supports the following weak server-to-client encryption al gorithm(s): 3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se
<b>Solution:</b> <b>Solution type:</b> Mitigation Disable the reported weak encryption algorithm(s).
<b>Vulnerability Insight</b> - 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.
... continues on next page ...

...continued from previous page ...
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.
<b>Vulnerability Detection Method</b> Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak encryption algorithms are defined as the following: - Arcfour (RC4) cipher based algorithms - 'none' algorithm - CBC mode cipher based algorithms Details: Weak Encryption Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105611 Version used: 2023-10-12T05:05:32Z
<b>References</b> url: <a href="https://www.rfc-editor.org/rfc/rfc8758">https://www.rfc-editor.org/rfc/rfc8758</a> url: <a href="https://www.kb.cert.org/vuls/id/958563">https://www.kb.cert.org/vuls/id/958563</a> url: <a href="https://www.rfc-editor.org/rfc/rfc4253#section-6.3">https://www.rfc-editor.org/rfc/rfc4253#section-6.3</a>

[ [return to 10.10.152.150](#) ]

### 2.1.6 Low general/icmp

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

...continued from previous page ...
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)
<b>Vulnerability Insight</b> The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.
<b>Vulnerability Detection Method</b> Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2023-05-11T09:09:33Z
<b>References</b> cve: CVE-1999-0524 url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a> cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658

[ [return to 10.10.152.150](#) ]

### 2.1.7 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection:</b> 80
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 496120228 Packet 2: 496120521
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
... continues on next page ...

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

[\[ return to 10.10.152.150 \]](#)

2.1.8 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)
<p><b>Summary</b></p> <p>This host is prone to an information disclosure vulnerability.</p>
... continues on next page ...



...continued from previous page ...
<b>Quality of Detection:</b> 80
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.
<b>Solution:</b> <b>Solution type:</b> Mitigation Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+
<b>Vulnerability Insight</b> The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code
<b>Vulnerability Detection Method</b> 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: 2023-07-26T05:05:09Z
<b>References</b> cve: CVE-2014-3566 url: <a href="https://www.openssl.org/~bodo/ssl-poodle.pdf">https://www.openssl.org/~bodo/ssl-poodle.pdf</a> url: <a href="http://www.securityfocus.com/bid/70574">http://www.securityfocus.com/bid/70574</a> url: <a href="https://www.imperialviolet.org/2014/10/14/poodle.html">https://www.imperialviolet.org/2014/10/14/poodle.html</a> url: <a href="https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html">https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html</a> url: <a href="http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin-↪g-ssl-30.html">http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploitin-↪g-ssl-30.html</a> 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
... continues on next page ...

...continued from previous page ...

cert-bund: CB-K15/1021  
cert-bund: CB-K15/0972  
cert-bund: CB-K15/0637  
cert-bund: CB-K15/0590  
cert-bund: CB-K15/0525  
cert-bund: CB-K15/0393  
cert-bund: CB-K15/0384  
cert-bund: CB-K15/0287  
cert-bund: CB-K15/0252  
cert-bund: CB-K15/0246  
cert-bund: CB-K15/0237  
cert-bund: CB-K15/0118  
cert-bund: CB-K15/0110  
cert-bund: CB-K15/0108  
cert-bund: CB-K15/0080  
cert-bund: CB-K15/0078  
cert-bund: CB-K15/0077  
cert-bund: CB-K15/0075  
cert-bund: CB-K14/1617  
cert-bund: CB-K14/1581  
cert-bund: CB-K14/1537  
cert-bund: CB-K14/1479  
cert-bund: CB-K14/1458  
cert-bund: CB-K14/1342  
cert-bund: CB-K14/1314  
cert-bund: CB-K14/1313  
cert-bund: CB-K14/1311  
cert-bund: CB-K14/1304  
cert-bund: CB-K14/1296  
dfn-cert: DFN-CERT-2017-1238  
dfn-cert: DFN-CERT-2017-1236  
dfn-cert: DFN-CERT-2016-1929  
dfn-cert: DFN-CERT-2016-1527  
dfn-cert: DFN-CERT-2016-1468  
dfn-cert: DFN-CERT-2016-1168  
dfn-cert: DFN-CERT-2016-0884  
dfn-cert: DFN-CERT-2016-0642  
dfn-cert: DFN-CERT-2016-0388  
dfn-cert: DFN-CERT-2016-0171  
dfn-cert: DFN-CERT-2015-1431  
dfn-cert: DFN-CERT-2015-1075  
dfn-cert: DFN-CERT-2015-1026  
dfn-cert: DFN-CERT-2015-0664  
dfn-cert: DFN-CERT-2015-0548  
dfn-cert: DFN-CERT-2015-0404  
dfn-cert: DFN-CERT-2015-0396  
dfn-cert: DFN-CERT-2015-0259

...continues on next page ...

...continued from previous page ...

```
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
```

[\[ return to 10.10.152.150 \]](#)**2.1.9 Low 2222/tcp**

Low (CVSS: 2.6)

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

**Summary**

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

**Quality of Detection: 80****Vulnerability Detection Result**The remote SSH server supports the following weak client-to-server MAC algorithm  $\hookrightarrow$ (s):

hmac-md5

hmac-md5-96

hmac-sha1-96

hmac-sha2-256-96

hmac-sha2-512-96

umac-64@openssh.com

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

hmac-md5

hmac-md5-96

hmac-sha1-96

hmac-sha2-256-96

... continues on next page ...

...continued from previous page ...	
hmac-sha2-512-96 umac-64@openssh.com	
<b>Solution:</b> <b>Solution type:</b> Mitigation Disable the reported weak MAC algorithm(s).	
<b>Vulnerability Detection Method</b> Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - 64-bit based algorithms - 'none' algorithm Details: Weak MAC Algorithm(s) Supported (SSH) OID:1.3.6.1.4.1.25623.1.0.105610 Version used: 2023-10-12T05:05:32Z	
<b>References</b> url: <a href="https://www.rfc-editor.org/rfc/rfc6668">https://www.rfc-editor.org/rfc/rfc6668</a> url: <a href="https://www.rfc-editor.org/rfc/rfc4253#section-6.4">https://www.rfc-editor.org/rfc/rfc4253#section-6.4</a>	

[ [return to 10.10.152.150](#) ]