

Scan Report

December 22, 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 “meta scan”. The scan started at Sun Dec 22 17:19:02 2024 UTC and ended at . The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

| | | |
|----------|----------------------------|----------|
| 1 | Result Overview | 2 |
| 2 | Results per Host | 2 |
| 2.1 | 192.168.187.128 | 2 |
| 2.1.1 | High 21/tcp | 3 |
| 2.1.2 | High 8787/tcp | 4 |
| 2.1.3 | High 3306/tcp | 5 |
| 2.1.4 | High 6200/tcp | 6 |
| 2.1.5 | High 5432/tcp | 7 |
| 2.1.6 | High 5900/tcp | 8 |
| 2.1.7 | High general/tcp | 9 |
| 2.1.8 | High 1524/tcp | 9 |
| 2.1.9 | High 80/tcp | 10 |
| 2.1.10 | High 512/tcp | 11 |
| 2.1.11 | High 6697/tcp | 12 |
| 2.1.12 | Medium 25/tcp | 14 |
| 2.1.13 | Medium 21/tcp | 27 |
| 2.1.14 | Medium 23/tcp | 29 |
| 2.1.15 | Medium 5432/tcp | 30 |
| 2.1.16 | Medium 5900/tcp | 44 |
| 2.1.17 | Medium 2121/tcp | 44 |
| 2.1.18 | Medium 80/tcp | 45 |

| | | |
|--------|-------------------------|----|
| 2.1.19 | Medium 22/tcp | 55 |
| 2.1.20 | Low 25/tcp | 58 |
| 2.1.21 | Low 5432/tcp | 63 |
| 2.1.22 | Low 22/tcp | 66 |

1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---------------------------------|------|--------|-----|-----|----------------|
| 192.168.187.128 | 12 | 32 | 4 | 0 | 0 |
| Total: 1 | 12 | 32 | 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 48 results selected by the filtering described above. Before filtering there were 585 results.

2 Results per Host

2.1 192.168.187.128

Host scan start Sun Dec 22 17:21:25 2024 UTC

Host scan end

| Service (Port) | Threat Level |
|-----------------------------|--------------|
| 21/tcp | High |
| 8787/tcp | High |
| 3306/tcp | High |
| 6200/tcp | High |
| 5432/tcp | High |
| 5900/tcp | High |
| general/tcp | High |
| 1524/tcp | High |
| 80/tcp | High |
| 512/tcp | High |
| 6697/tcp | High |
| 25/tcp | Medium |
| 21/tcp | Medium |
| 23/tcp | Medium |
| 5432/tcp | Medium |
| 5900/tcp | Medium |

... (continues) ...

... (continued) ...

| Service (Port) | Threat Level |
|----------------|--------------|
| 2121/tcp | Medium |
| 80/tcp | Medium |
| 22/tcp | Medium |
| 25/tcp | Low |
| 5432/tcp | Low |
| 22/tcp | Low |

2.1.1 High 21/tcp

| |
|---|
| High (CVSS: 9.8) |
| NVT: vsftpd Compromised Source Packages Backdoor Vulnerability |
| Summary vsftpd is prone to a backdoor vulnerability. |
| Quality of Detection (QoD): 99% |
| Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method. |
| Impact Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application. |
| Solution: Solution type: VendorFix The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature. |
| Affected Software/OS The vsftpd 2.3.4 source package downloaded between 20110630 and 20110703 is affected. |
| Vulnerability Insight The tainted source package contains a backdoor which opens a shell on port 6200/tcp. |
| Vulnerability Detection Method Details: vsftpd Compromised Source Packages Backdoor Vulnerability OID:1.3.6.1.4.1.25623.1.0.103185 Version used: 2023-12-07T05:05:41Z |
| References cve: CVE-2011-2523 |
| ... continues on next page ... |

| |
|--|
| ...continued from previous page ... |
| url: https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html |
| url: https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bid/48539/ |
| url: https://security.appspot.com/vsftpd.html |

[\[return to 192.168.187.128 \]](#)

2.1.2 High 8787/tcp

| |
|--|
| High (CVSS: 10.0) |
| NVT: Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities |
| <p>Summary</p> <p>Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.</p> |
| <p>Quality of Detection (QoD): 99%</p> |
| <p>Vulnerability Detection Result</p> <p>The service is running in \$SAFE >= 1 mode. However it is still possible to run a arbitrary syscall commands on the remote host. Sending an invalid syscall the service returned the following response:</p> <pre>Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in 'syscall'"0/usr/lib/ruby/1.8/drb/drb.rb:1555:in 'send'"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in '__send__'"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in 'perform_without_block'"3/usr/lib/ruby/1.8/drb/drb.rb:1515:in 'perform'"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in 'main_loop'"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in 'loop'"5/usr/lib/ruby/1.8/drb/drb.rb:1585:in 'main_loop'"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in 'start'"5/usr/lib/ruby/1.8/drb/drb.rb:1581:in 'main_loop'"/usr/lib/ruby/1.8/drb/drb.rb:143:in 'run'"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in 'start'"/usr/lib/ruby/1.8/drb/drb.rb:1427:in 'run'"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in 'initialize'"/usr/lib/ruby/1.8/drb/drb.rb:1627:in 'new'"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in 'start_service'"/usr/sbin/druby_timeserver.rb:12:errno+:mesg"Function not implemented</pre> |
| <p>Impact</p> <p>By default, Distributed Ruby does not impose restrictions on allowed hosts or set the \$SAFE environment variable to prevent privileged activities. If other controls are not in place, especially if the Distributed Ruby process runs with elevated privileges, an attacker could execute arbitrary system commands or Ruby scripts on the Distributed Ruby server. An attacker may need to know only the URI of the listening Distributed Ruby server to submit Ruby commands.</p> |
| <p>Solution:</p> <p>... continues on next page ...</p> |

| |
|--|
| ...continued from previous page ... |
| <p>Solution type: Mitigation</p> <p>Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include:</p> <ul style="list-style-type: none">- Implementing taint on untrusted input- Setting \$SAFE levels appropriately (≥ 2 is recommended if untrusted hosts are allowed to submit Ruby commands, and ≥ 3 may be appropriate)- Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts |
| <p>Vulnerability Detection Method</p> <p>Send a crafted command to the service and check for a remote command execution via the instance_eval or syscall requests.</p> <p>Details: Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities</p> <p>OID:1.3.6.1.4.1.25623.1.0.108010</p> <p>Version used: 2024-06-28T05:05:33Z</p> |
| <p>References</p> <p>url: https://tools.cisco.com/security/center/viewAlert.x?alertId=22750</p> <p>url: http://www.securityfocus.com/bid/47071</p> <p>url: http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_testing/</p> <p>url: http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html</p> |

[\[return to 192.168.187.128 \]](#)

2.1.3 High 3306/tcp

| |
|---|
| High (CVSS: 9.8) |
| NVT: MySQL / MariaDB Default Credentials (MySQL Protocol) |
| <p>Summary</p> <p>It was possible to login into the remote MySQL as root using weak credentials.</p> |
| <p>Quality of Detection (QoD): 95%</p> |
| <p>Vulnerability Detection Result</p> <p>It was possible to login as root with an empty password.</p> |
| <p>Solution:</p> <p>Solution type: Mitigation</p> <ul style="list-style-type: none">- Change the password as soon as possible- Contact the vendor for other possible fixes / updates |
| ... continues on next page ... |

...continued from previous page ...

Affected Software/OS

The following products are known to use such weak credentials:

- CVE-2001-0645: Symantec/AXENT NetProwler 3.5.x
- CVE-2004-2357: Proofpoint Protection Server
- CVE-2006-1451: MySQL Manager in Apple Mac OS X 10.3.9 and 10.4.6
- CVE-2007-2554: Associated Press (AP) Newspaper 4.0.1 and earlier
- CVE-2007-6081: AdventNet EventLog Analyzer build 4030
- CVE-2009-0919: XAMPP
- CVE-2014-3419: Infoblox NetMRI before 6.8.5
- CVE-2015-4669: Xsuite 2.x
- CVE-2016-6531, CVE-2018-15719: Open Dental before version 18.4

Other products might be affected as well.

Vulnerability Detection Method

Details: MySQL / MariaDB Default Credentials (MySQL Protocol)

OID:1.3.6.1.4.1.25623.1.0.103551

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

References

- cve: CVE-2001-0645
- cve: CVE-2004-2357
- cve: CVE-2006-1451
- cve: CVE-2007-2554
- cve: CVE-2007-6081
- cve: CVE-2009-0919
- cve: CVE-2014-3419
- cve: CVE-2015-4669
- cve: CVE-2016-6531
- cve: CVE-2018-15719

[\[return to 192.168.187.128 \]](#)

2.1.4 High 6200/tcp

High (CVSS: 9.8)

NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Summary

vsftpd is prone to a backdoor vulnerability.

Quality of Detection (QoD): 99%

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

...continued from previous page ...

Impact

Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Solution:

Solution type: VendorFix

The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature.

Affected Software/OS

The vsftpd 2.3.4 source package downloaded between 20110630 and 20110703 is affected.

Vulnerability Insight

The tainted source package contains a backdoor which opens a shell on port 6200/tcp.

Vulnerability Detection Method

Details: vsftpd Compromised Source Packages Backdoor Vulnerability

OID:1.3.6.1.4.1.25623.1.0.103185

Version used: 2023-12-07T05:05:41Z

References

cve: CVE-2011-2523

url: <https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html>

url: <https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bid/48539/>

url: <https://security.appspot.com/vsftpd.html>

[\[return to 192.168.187.128 \]](#)

2.1.5 High 5432/tcp

High (CVSS: 9.0)

NVT: PostgreSQL Default Credentials (PostgreSQL Protocol)

Summary

It was possible to login into the remote PostgreSQL as user postgres using weak credentials.

Quality of Detection (QoD): 99%

Vulnerability Detection Result

It was possible to login as user postgres with password "postgres".

... continues on next page ...

...continued from previous page ...

Solution:

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Details: PostgreSQL Default Credentials (PostgreSQL Protocol)

OID:1.3.6.1.4.1.25623.1.0.103552

Version used: 2024-07-19T15:39:06Z

[\[return to 192.168.187.128 \]](#)

2.1.6 High 5900/tcp

High (CVSS: 9.0)

NVT: VNC Brute Force Login

Summary

Try to log in with given passwords via VNC protocol.

Quality of Detection (QoD): 95%

Vulnerability Detection Result

It was possible to connect to the VNC server with the password: password

Solution:

Solution type: Mitigation

Change the password to something hard to guess or enable password protection at all.

Vulnerability Insight

This script tries to authenticate to a VNC server with the passwords set in the password preference. It will also test and report if no authentication / password is required at all.

Note: Some VNC servers have a blacklisting scheme that blocks IP addresses after five unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked.

Note as well that passwords can be max. 8 characters long.

Vulnerability Detection Method

Details: VNC Brute Force Login

OID:1.3.6.1.4.1.25623.1.0.106056

Version used: 2021-07-23T07:56:26Z

[\[return to 192.168.187.128 \]](#)

2.1.7 High general/tcp

| |
|--|
| High (CVSS: 10.0) |
| NVT: Operating System (OS) End of Life (EOL) Detection |
| Summary The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore. |
| Quality of Detection (QoD): 80% |
| Vulnerability Detection Result The "Ubuntu" Operating System on the remote host has reached the end of life. CPE: cpe:/o:canonical:ubuntu_linux:8.04 Installed version, build or SP: 8.04 EOL date: 2013-05-09 EOL info: https://wiki.ubuntu.com/Releases |
| Impact 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. |
| Solution: Solution type: Mitigation Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor. |
| Vulnerability Detection Method Checks if an EOL version of an OS is present on the target host. Details: Operating System (OS) End of Life (EOL) Detection OID:1.3.6.1.4.1.25623.1.0.103674 Version used: 2024-02-28T14:37:42Z |

[\[return to 192.168.187.128 \]](#)

2.1.8 High 1524/tcp

| |
|--|
| High (CVSS: 10.0) |
| NVT: Possible Backdoor: Ingreslock |
| Summary ... continues on next page ... |

| |
|--|
| ...continued from previous page ... |
| A backdoor is installed on the remote host. |
| Quality of Detection (QoD): 99% |
| Vulnerability Detection Result The service is answering to an 'id;' command with the following response: uid=0(↪root) gid=0(root) |
| Impact Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem. |
| Solution: Solution type: Workaround A whole cleanup of the infected system is recommended. |
| Vulnerability Detection Method Details: Possible Backdoor: Ingreslock OID:1.3.6.1.4.1.25623.1.0.103549 Version used: 2023-07-25T05:05:58Z |

[\[return to 192.168.187.128 \]](#)

2.1.9 High 80/tcp

| |
|---|
| High (CVSS: 10.0) |
| NVT: TWiki XSS and Command Execution Vulnerabilities |
| Summary TWiki is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities. |
| Quality of Detection (QoD): 80% |
| Vulnerability Detection Result Installed version: 01.Feb.2003 Fixed version: 4.2.4 |
| Impact Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application. |
| Solution: Solution type: VendorFix |
| ... continues on next page ... |

| |
|---|
| ...continued from previous page ... |
| Upgrade to version 4.2.4 or later. |
| Affected Software/OS TWiki, TWiki version prior to 4.2.4. |
| Vulnerability Insight The flaws are due to: - %URLPARAM}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack. - %SEARCH}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack. |
| Vulnerability Detection Method Details: TWiki XSS and Command Execution Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.800320 Version used: 2024-03-01T14:37:10Z |
| References cve: CVE-2008-5304 cve: CVE-2008-5305 url: http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304 url: http://www.securityfocus.com/bid/32668 url: http://www.securityfocus.com/bid/32669 url: http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305 |

[[return to 192.168.187.128](#)]

2.1.10 High 512/tcp

| |
|--|
| High (CVSS: 10.0) NVT: The rexec service is running |
| Summary This remote host is running a rexec service. |
| Quality of Detection (QoD): 80% |
| Vulnerability Detection Result The rexec service was detected on the target system. |
| Solution: Solution type: Mitigation Disable the rexec service and use alternatives like SSH instead. |
| ... continues on next page ... |

...continued from previous page ...

Vulnerability Insight

rexec (remote execution client for an exec server) has the same kind of functionality that rsh has: you can execute shell commands on a remote computer.

The main difference is that rexec authenticates by reading the username and password *unencrypted* from the socket.

Vulnerability Detection Method

Checks whether an rexec service is exposed on the target host.

Details: **The rexec service is running**

OID:1.3.6.1.4.1.25623.1.0.100111

Version used: 2023-09-12T05:05:19Z

References

cve: CVE-1999-0618

[\[return to 192.168.187.128 \]](#)

2.1.11 High 6697/tcp

High (CVSS: 8.1)

NVT: UnrealIRCd Authentication Spoofing Vulnerability

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.

... continues on next page ...

| |
|---|
| ...continued from previous page ... |
| 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 |
| 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 |
| 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 Remote attackers can exploit this issue to execute arbitrary system commands within the context of the affected application. |
| ... continues on next page ... |

...continued from previous page ...

Vulnerability Detection Method

Details: UnrealIRCd Backdoor

OID:1.3.6.1.4.1.25623.1.0.80111

Version used: 2023-08-01T13:29:10Z

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>[\[return to 192.168.187.128 \]](#)**2.1.12 Medium 25/tcp**

Medium (CVSS: 5.9)

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

Summary

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

Quality of Detection (QoD): 98%**Vulnerability Detection Result**

In addition to TLSv1.0+ the service is also providing the deprecated SSLv2 and SSLv3 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

Impact

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

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

Solution:**Solution type:** Mitigation

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

Affected Software/OS

... continues on next page ...

| |
|--|
| ...continued from previous page ... |
| All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols. |
| Vulnerability Insight The SSLv2 and SSLv3 protocols contain known cryptographic flaws like: - CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE) - CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN) |
| Vulnerability Detection Method Check the used SSL protocols of the services provided by this system. Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.111012 Version used: 2024-09-27T05:05:23Z |
| References cve: CVE-2016-0800 cve: CVE-2014-3566 url: https://ssl-config.mozilla.org/ url: https://bettercrypto.org/ url: https://drownattack.com/ url: https://www.imperialviolet.org/2014/10/14/poodle.html url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters ↔-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 |
| ... continues on next page ... |

...continued from previous page ...

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
 dfn-cert: DFN-CERT-2016-0644
 dfn-cert: DFN-CERT-2016-0642
 dfn-cert: DFN-CERT-2016-0496
 dfn-cert: DFN-CERT-2016-0495

...continues on next page ...

...continued from previous page ...

```

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

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%

... continues on next page ...

| | |
|---|--|
| ...continued from previous page... | |
| Vulnerability Detection Result The remote SSL/TLS server is using the following certificate(s) with a RSA key with less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer): 1024:RSA:00FAF93A4C7FB6B9CC:1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,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 (Server certificate) | |
| Impact Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information. | |
| Solution: Solution type: Mitigation Replace the certificate with a stronger key and reissue the certificates it signed. | |
| Vulnerability Insight SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe. | |
| Vulnerability Detection Method Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit. Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048. ↪.. OID:1.3.6.1.4.1.25623.1.0.150710 Version used: 2021-12-10T12:48:00Z | |
| References url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf | |
| Medium (CVSS: 5.0) NVT: SSL/TLS: Certificate Expired | |
| Summary The remote server's SSL/TLS certificate has already expired. | |
| Quality of Detection (QoD): 99% | |
| Vulnerability Detection Result 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 | |
| ... continues on next page ... | |

| | |
|--|---|
| ...continued from previous page... | |
| issued by | 1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office ↪ for Complication of Otherwise Simple Affairs,0=OC0SA,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,0=OC0SA,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 |
| 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 | |

| |
|--|
| 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'. ... continues on next page ... |

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

| |
|--|
| <p>Medium (CVSS: 4.3)</p> <p>NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection</p> |
| <p>Summary</p> <p>It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.</p> |
| <p>Quality of Detection (QoD): 98%</p> |
| <p>Vulnerability Detection Result</p> <p>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.</p> |
| <p>Impact</p> <p>An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.</p> <p>Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.</p> |
| <p>Solution:</p> <p>Solution type: Mitigation</p> <p>It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.</p> |
| <p>Affected Software/OS</p> <p>... continues on next page ...</p> |

| |
|--|
| ...continued from previous page ... |
| All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols. |
| Vulnerability Insight The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK) |
| Vulnerability Detection Method Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2024-09-27T05:05:23Z |
| References cve: CVE-2011-3389 cve: CVE-2015-0204 url: https://ssl-config.mozilla.org/ url: https://bettercrypto.org/ url: https://datatracker.ietf.org/doc/rfc8996/ url: https://vnhacker.blogspot.com/2011/09/beast.html url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters ↔-report-2014 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K18/0799 cert-bund: CB-K16/1289 cert-bund: CB-K16/1096 cert-bund: CB-K15/1751 cert-bund: CB-K15/1266 cert-bund: CB-K15/0850 cert-bund: CB-K15/0764 cert-bund: CB-K15/0720 cert-bund: CB-K15/0548 cert-bund: CB-K15/0526 cert-bund: CB-K15/0509 cert-bund: CB-K15/0493 cert-bund: CB-K15/0384 cert-bund: CB-K15/0365 cert-bund: CB-K15/0364 cert-bund: CB-K15/0302 cert-bund: CB-K15/0192 cert-bund: CB-K15/0079 cert-bund: CB-K15/0016 cert-bund: CB-K14/1342 cert-bund: CB-K14/0231 cert-bund: CB-K13/0845 |
| ... continues on next page ... |

| | |
|-------------------------------------|--------------------|
| ...continued from previous page ... | |
| cert-bund: | CB-K13/0796 |
| cert-bund: | CB-K13/0790 |
| dfn-cert: | DFN-CERT-2020-0177 |
| dfn-cert: | DFN-CERT-2020-0111 |
| dfn-cert: | DFN-CERT-2019-0068 |
| dfn-cert: | DFN-CERT-2018-1441 |
| dfn-cert: | DFN-CERT-2018-1408 |
| dfn-cert: | DFN-CERT-2016-1372 |
| dfn-cert: | DFN-CERT-2016-1164 |
| dfn-cert: | DFN-CERT-2016-0388 |
| dfn-cert: | DFN-CERT-2015-1853 |
| dfn-cert: | DFN-CERT-2015-1332 |
| dfn-cert: | DFN-CERT-2015-0884 |
| dfn-cert: | DFN-CERT-2015-0800 |
| dfn-cert: | DFN-CERT-2015-0758 |
| dfn-cert: | DFN-CERT-2015-0567 |
| dfn-cert: | DFN-CERT-2015-0544 |
| dfn-cert: | DFN-CERT-2015-0530 |
| dfn-cert: | DFN-CERT-2015-0396 |
| dfn-cert: | DFN-CERT-2015-0375 |
| dfn-cert: | DFN-CERT-2015-0374 |
| dfn-cert: | DFN-CERT-2015-0305 |
| dfn-cert: | DFN-CERT-2015-0199 |
| dfn-cert: | DFN-CERT-2015-0079 |
| dfn-cert: | DFN-CERT-2015-0021 |
| dfn-cert: | DFN-CERT-2014-1414 |
| dfn-cert: | DFN-CERT-2013-1847 |
| dfn-cert: | DFN-CERT-2013-1792 |
| dfn-cert: | DFN-CERT-2012-1979 |
| dfn-cert: | DFN-CERT-2012-1829 |
| dfn-cert: | DFN-CERT-2012-1530 |
| dfn-cert: | DFN-CERT-2012-1380 |
| dfn-cert: | DFN-CERT-2012-1377 |
| dfn-cert: | DFN-CERT-2012-1292 |
| dfn-cert: | DFN-CERT-2012-1214 |
| dfn-cert: | DFN-CERT-2012-1213 |
| dfn-cert: | DFN-CERT-2012-1180 |
| dfn-cert: | DFN-CERT-2012-1156 |
| dfn-cert: | DFN-CERT-2012-1155 |
| dfn-cert: | DFN-CERT-2012-1039 |
| dfn-cert: | DFN-CERT-2012-0956 |
| dfn-cert: | DFN-CERT-2012-0908 |
| dfn-cert: | DFN-CERT-2012-0868 |
| dfn-cert: | DFN-CERT-2012-0867 |
| dfn-cert: | DFN-CERT-2012-0848 |
| dfn-cert: | DFN-CERT-2012-0838 |
| dfn-cert: | DFN-CERT-2012-0776 |
| ... continues on next page ... | |

...continued from previous page ...

```

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

Summary

This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

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

... continues on next page ...

| |
|--|
| ...continued from previous page ... |
| <p>'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:</p> <pre>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</pre> |
| <p>Impact</p> <p>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.</p> |
| <p>Solution:</p> <p>Solution type: VendorFix</p> <ul style="list-style-type: none"> - Remove support for 'RSA_EXPORT' cipher suites from the service. - If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later. |
| <p>Affected Software/OS</p> <ul style="list-style-type: none"> - Hosts accepting 'RSA_EXPORT' cipher suites - OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k. |
| <p>Vulnerability Insight</p> <p>Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.</p> |
| <p>Vulnerability Detection Method</p> <p>Check previous collected cipher suites saved in the KB.</p> <p>Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)</p> <p>OID:1.3.6.1.4.1.25623.1.0.805142</p> <p>Version used: 2024-09-30T08:38:05Z</p> |
| <p>References</p> <p>cve: CVE-2015-0204</p> <p>url: https://freakattack.com</p> <p>url: http://www.securityfocus.com/bid/71936</p> <p>url: http://secpod.org/blog/?p=3818</p> <p>url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html</p> <p>cert-bund: CB-K18/0799</p> <p>cert-bund: CB-K16/1289</p> <p>cert-bund: CB-K16/1096</p> <p>cert-bund: CB-K15/1751</p> <p>cert-bund: CB-K15/1266</p> <p>cert-bund: CB-K15/0850</p> <p>cert-bund: CB-K15/0764</p> <p>cert-bund: CB-K15/0720</p> |
| ... continues on next page ... |

...continued from previous page ...

```

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

```

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

... continues on next page ...

| |
|--|
| ...continued from previous page ... |
| <p>Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).</p> <p>For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.</p> |
| <p>Vulnerability Insight</p> <p>The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.</p> |
| <p>Vulnerability Detection Method</p> <p>Checks the DHE temporary public key size.</p> <p>Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability. ↪...</p> <p>OID:1.3.6.1.4.1.25623.1.0.106223</p> <p>Version used: 2024-09-30T08:38:05Z</p> |
| <p>References</p> <p>url: https://weakdh.org/</p> <p>url: https://weakdh.org/sysadmin.html</p> |

| |
|---|
| Medium (CVSS: 4.0) |
| NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm |
| <p>Summary</p> <p>The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.</p> |
| <p>Quality of Detection (QoD): 80%</p> |
| <p>Vulnerability Detection Result</p> <p>The following certificates are part of the certificate chain but using insecure ↪signature algorithms:</p> <p>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</p> <p>Signature Algorithm: sha1WithRSAEncryption</p> |
| <p>Solution:</p> <p>Solution type: Mitigation</p> |
| ... continues on next page ... |

| |
|--|
| ...continued from previous page ... |
| 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>Vulnerability Insight</p> <p>The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:</p> <ul style="list-style-type: none"> - Secure Hash Algorithm 1 (SHA-1) - Message Digest 5 (MD5) - Message Digest 4 (MD4) - Message Digest 2 (MD2) <p>Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.</p> <p>NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:</p> <p>Fingerprint1 or fingerprint1, Fingerprint2</p> |
| <p>Vulnerability Detection Method</p> <p>Check which hashing algorithm was used to sign the remote SSL/TLS certificate.</p> <p>Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm</p> <p>OID:1.3.6.1.4.1.25623.1.0.105880</p> <p>Version used: 2021-10-15T11:13:32Z</p> |
| <p>References</p> <p>url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/</p> |

[[return to 192.168.187.128](#)]

2.1.13 Medium 21/tcp

| |
|--|
| Medium (CVSS: 6.4) |
| NVT: Anonymous FTP Login Reporting |
| <p>Summary</p> <p>Reports if the remote FTP Server allows anonymous logins.</p> |
| Quality of Detection (QoD): 80% |
| ... continues on next page ... |

| |
|---|
| ...continued from previous page... |
| 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 |
| Impact Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to: - gain access to sensitive files - upload or delete files. |
| Solution: Solution type: Mitigation If you do not want to share files, you should disable anonymous logins. |
| Vulnerability Insight A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data. Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target. |
| Vulnerability Detection Method Details: Anonymous FTP Login Reporting OID:1.3.6.1.4.1.25623.1.0.900600 Version used: 2021-10-20T09:03:29Z |
| References cve: CVE-1999-0497 |

Medium (CVSS: 4.8)

NVT: FTP Unencrypted Cleartext Login

Summary

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

Quality of Detection (QoD): 70%

Vulnerability Detection Result

... continues on next page ...

| |
|---|
| ...continued from previous page ... |
| <p>The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↔. Response(s):</p> <p>Non-anonymous sessions: 331 Please specify the password.</p> <p>Anonymous sessions: 331 Please specify the password.</p> |
| <p>Impact</p> <p>An attacker can uncover login names and passwords by sniffing traffic to the FTP service.</p> |
| <p>Solution:</p> <p>Solution type: Mitigation</p> <p>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</p> <p>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.</p> <p>Details: FTP Unencrypted Cleartext Login</p> <p>OID:1.3.6.1.4.1.25623.1.0.108528</p> <p>Version used: 2023-12-20T05:05:58Z</p> |

[\[return to 192.168.187.128 \]](#)

2.1.14 Medium 23/tcp

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

...continued from previous page ...

Vulnerability Detection Method

Details: Telnet Unencrypted Cleartext Login

OID:1.3.6.1.4.1.25623.1.0.108522

Version used: 2023-10-13T05:06:09Z

[\[return to 192.168.187.128 \]](#)**2.1.15 Medium 5432/tcp**

Medium (CVSS: 5.9)

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

Summary

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

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 information.

Affected Software/OS

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

Vulnerability Insight

The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:

... continues on next page ...

| |
|---|
| ...continued from previous page ... |
| <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) |
| <p>Vulnerability Detection Method</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: 2024-09-27T05:05:23Z</p> |
| <p>References</p> <p>cve: CVE-2016-0800 cve: CVE-2014-3566 url: https://ssl-config.mozilla.org/ url: https://bettercrypto.org/ url: https://drownattack.com/ url: https://www.imperialviolet.org/2014/10/14/poodle.html url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters ↔-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 cert-bund: CB-K15/1021</p> |
| ...continues on next page ... |

...continued from previous page ...

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
dfn-cert: DFN-CERT-2016-0451

...continues on next page ...

...continued from previous page ...

```

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: 5.9)

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 (QoD): 98%**Vulnerability Detection Result**

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

...continues on next page ...

| |
|--|
| ...continued from previous page ... |
| <p>TLS_RSA_WITH_RC4_128_SHA</p> <p>'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:</p> <p>TLS_RSA_WITH_RC4_128_SHA</p> |
| <p>Solution:</p> <p>Solution type: Mitigation</p> <p>The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.</p> <p>Please see the references for more resources supporting you with this task.</p> |
| <p>Vulnerability Insight</p> <p>These rules are applied for the evaluation of the cryptographic strength:</p> <ul style="list-style-type: none"> - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808) - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000) - 1024 bit RSA authentication is considered to be insecure and therefore as weak - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong |
| <p>Vulnerability Detection Method</p> <p>Details: SSL/TLS: Report Weak Cipher Suites</p> <p>OID:1.3.6.1.4.1.25623.1.0.103440</p> <p>Version used: 2024-09-27T05:05:23Z</p> |
| <p>References</p> <p>cve: CVE-2013-2566</p> <p>cve: CVE-2015-2808</p> <p>cve: CVE-2015-4000</p> <p>url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1↪465_update_6.html</p> <p>url: https://bettercrypto.org/</p> <p>url: https://mozilla.github.io/server-side-tls/ssl-config-generator/</p> <p>cert-bund: CB-K21/0067</p> <p>cert-bund: CB-K19/0812</p> <p>cert-bund: CB-K17/1750</p> <p>cert-bund: CB-K16/1593</p> <p>cert-bund: CB-K16/1552</p> <p>cert-bund: CB-K16/1102</p> <p>cert-bund: CB-K16/0617</p> <p>cert-bund: CB-K16/0599</p> <p>cert-bund: CB-K16/0168</p> <p>cert-bund: CB-K16/0121</p> <p>cert-bund: CB-K16/0090</p> <p>cert-bund: CB-K16/0030</p> <p>cert-bund: CB-K15/1751</p> <p>cert-bund: CB-K15/1591</p> |
| ... continues on next page ... |

...continued from previous page ...

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
dfn-cert: DFN-CERT-2016-0035

...continues on next page ...

...continued from previous page ...

```

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**

The remote SSL/TLS server is using the following certificate(s) with a RSA key w
...continues on next page ...

| |
|---|
| ...continued from previous page ... |
| <pre> ↪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 ↪omplication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no su ↪ch thing outside US,C=XX (Server certificate) </pre> |
| Impact Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information. |
| Solution: Solution type: Mitigation Replace the certificate with a stronger key and reissue the certificates it signed. |
| Vulnerability Insight SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe. |
| Vulnerability Detection Method Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit. Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048. ↪.. OID:1.3.6.1.4.1.25623.1.0.150710 Version used: 2021-12-10T12:48:00Z |
| References url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf |

Medium (CVSS: 5.0)

NVT: SSL/TLS: Certificate Expired

Summary

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

Quality of Detection (QoD): 99%**Vulnerability Detection Result**

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

... continues on next page ...

| | |
|--|--|
| ...continued from previous page... | |
| ↪ for Complication of Otherwise Simple Affairs,0=OC0SA,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,0=OC0SA,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 |
| 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 | |

| |
|---|
| 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 (QoD): 98% |
| Vulnerability Detection Result |
| The service is only providing the deprecated TLSv1.0 protocol and supports one o ↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S ↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT. |
| Impact |
| ... continues on next page ... |

| |
|---|
| ...continued from previous page ... |
| <p>An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.</p> <p>Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.</p> |
| <p>Solution:</p> <p>Solution type: Mitigation</p> <p>It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.</p> |
| <p>Affected Software/OS</p> <p>All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.</p> |
| <p>Vulnerability Insight</p> <p>The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:</p> <ul style="list-style-type: none"> - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK) |
| <p>Vulnerability Detection Method</p> <p>Check the used TLS protocols of the services provided by this system.</p> <p>Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection</p> <p>OID:1.3.6.1.4.1.25623.1.0.117274</p> <p>Version used: 2024-09-27T05:05:23Z</p> |
| <p>References</p> <p>cve: CVE-2011-3389</p> <p>cve: CVE-2015-0204</p> <p>url: https://ssl-config.mozilla.org/</p> <p>url: https://bettercrypto.org/</p> <p>url: https://datatracker.ietf.org/doc/rfc8996/</p> <p>url: https://vnhacker.blogspot.com/2011/09/beast.html</p> <p>url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak</p> <p>url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters</p> <p>↔-report-2014</p> <p>cert-bund: WID-SEC-2023-1435</p> <p>cert-bund: CB-K18/0799</p> <p>cert-bund: CB-K16/1289</p> <p>cert-bund: CB-K16/1096</p> <p>cert-bund: CB-K15/1751</p> <p>cert-bund: CB-K15/1266</p> <p>cert-bund: CB-K15/0850</p> <p>cert-bund: CB-K15/0764</p> <p>cert-bund: CB-K15/0720</p> <p>cert-bund: CB-K15/0548</p> |
| ... continues on next page ... |

...continued from previous page ...

cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292

...continues on next page ...

...continued from previous page...

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: 4.0) |
| 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 Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits. |
| Vulnerability Insight The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments. |
| 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: 2024-09-30T08:38:05Z |
| References url: https://weakdh.org/ url: https://weakdh.org/sysadmin.html |

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

| |
|--|
| ...continued from previous page ... |
| The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm. |
| 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 Complic ↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi ↪ng outside US,C=XX Signature Algorithm: sha1WithRSAEncryption |
| Solution: Solution type: Mitigation Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings. |
| Vulnerability Insight The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use: - Secure Hash Algorithm 1 (SHA-1) - Message Digest 5 (MD5) - Message Digest 4 (MD4) - Message Digest 2 (MD2) Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates. NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive: Fingerprint1 or fingerprint1, Fingerprint2 |
| Vulnerability Detection Method Check which hashing algorithm was used to sign the remote SSL/TLS certificate. Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm OID:1.3.6.1.4.1.25623.1.0.105880 Version used: 2021-10-15T11:13:32Z |
| References url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/ |

[\[return to 192.168.187.128 \]](#)

2.1.16 Medium 5900/tcp

| |
|--|
| Medium (CVSS: 4.8) |
| NVT: VNC Server Unencrypted Data Transmission |
| 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. |
| Quality of Detection (QoD): 70% |
| Vulnerability Detection Result The VNC server provides the following insecure or cryptographically weak Security Type(s): 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 |

[\[return to 192.168.187.128 \]](#)

2.1.17 Medium 2121/tcp

| |
|--------------------------------------|
| Medium (CVSS: 4.8) |
| NVT: FTP Unencrypted Cleartext Login |
| ... continues on next page ... |

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

[\[return to 192.168.187.128 \]](#)

2.1.18 Medium 80/tcp

| |
|---|
| Medium (CVSS: 6.8) |
| NVT: TWiki Cross-Site Request Forgery Vulnerability (Sep 2010) |
| 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: 4.3.2 |
| ... continues on next page ... |

| |
|---|
| ...continued from previous page ... |
| 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 TWiki version 4.3.2 or later. |
| 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 cve: CVE-2009-4898 url: http://www.openwall.com/lists/oss-security/2010/08/03/8 url: http://www.openwall.com/lists/oss-security/2010/08/02/17 url: http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix 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://192.168.187.128/mutillidae/javascript/ddsmoothmenu/jqu ... continues on next page ... |

| | |
|--|--|
| ...continued from previous page ... | |
| ↪ery.min.js - Referenced at: http://192.168.187.128/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 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-2023-1197 dfn-cert: DFN-CERT-2020-0590 | |
| 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 | |
| ... continues on next page ... | |

| |
|--|
| ...continued from previous page ... |
| 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 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: 6.0) |
| 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 |
| ... continues on next page ... |

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

...continued from previous page ...

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

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-trace-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://192.168.187.128/mutillidae/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 Variables</h2></pre> http://192.168.187.128/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 Variables</h2></pre> |
| Impact Some of the information that can be gathered from this file includes: 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. |
| Solution: Solution type: Workaround Delete the listed files or restrict access to them. |
| Affected Software/OS All systems exposing a file containing the output of the phpinfo() PHP function. This VT is also reporting if an affected endpoint for the following products have been identified: - CVE-2008-0149: TUTOS - CVE-2023-49282, CVE-2023-49283: Microsoft Graph PHP SDK |
| Vulnerability Insight ... continues on next page ... |

| |
|--|
| ...continued from previous page ... |
| Many PHP installation tutorials instruct the user to create a file called <code>phpinfo.php</code> or similar containing the <code>phpinfo()</code> statement. Such a file is often left back in the webserver directory. |
| Vulnerability Detection Method 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). Details: <code>phpinfo()</code> Output Reporting (HTTP) OID:1.3.6.1.4.1.25623.1.0.11229 Version used: 2024-12-17T05:05:41Z |
| References cve: CVE-2008-0149 cve: CVE-2023-49282 cve: CVE-2023-49283 url: https://www.php.net/manual/en/function.phpinfo.php |

| |
|--|
| Medium (CVSS: 5.0) |
| NVT: <code>/doc directory browsable</code> |
| Summary The <code>/doc</code> directory is browsable. <code>/doc</code> shows the content of the <code>/usr/doc</code> directory and therefore it shows which programs and - important! - the version of the installed programs. |
| Quality of Detection (QoD): 80% |
| Vulnerability Detection Result Vulnerable URL: <code>http://192.168.187.128/doc/</code> |
| Solution: Solution type: Mitigation Use access restrictions for the <code>/doc</code> directory. If you use Apache you might use this in your <code>access.conf</code> : <code><Directory /usr/doc> AllowOverride None order deny, allow deny from all allow from localhost </Directory></code> |
| Vulnerability Detection Method Details: <code>/doc directory browsable</code> OID:1.3.6.1.4.1.25623.1.0.10056 Version used: 2023-08-01T13:29:10Z |
| References cve: CVE-1999-0678 url: http://www.securityfocus.com/bid/318 |

| |
|--|
| Medium (CVSS: 4.8) |
| NVT: Cleartext Transmission of Sensitive Information via HTTP |
| Summary The host / application transmits sensitive information (username, passwords) in cleartext via HTTP. |
| Quality of Detection (QoD): 80% |
| Vulnerability Detection Result The following input fields were identified (URL:input name): http://192.168.187.128/dvwa/login.php:password http://192.168.187.128/phpMyAdmin/:pma_password http://192.168.187.128/phpMyAdmin/?D=A:pma_password http://192.168.187.128/tikiwiki/tiki-install.php:pass http://192.168.187.128/twiki/bin/view/TWiki/TWikiUserAuthentication:oldpassword |
| Impact An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords. |
| Solution: Solution type: Workaround Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions. |
| Affected Software/OS Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection. |
| Vulnerability Detection Method Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection. The script is currently checking the following: - HTTP Basic Authentication (Basic Auth) - HTTP Forms (e.g. Login) with input field of type 'password' Details: Cleartext Transmission of Sensitive Information via HTTP OID:1.3.6.1.4.1.25623.1.0.108440 Version used: 2023-09-07T05:05:21Z |
| References url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management ↪ssion_Management |
| ... continues on next page ... |

...continued from previous page...

url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: <https://cwe.mitre.org/data/definitions/319.html>

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://192.168.187.128/mutillidae/javascript/ddsmoothmenu/jquery.min.js>

- Referenced at: <http://192.168.187.128/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

[\[return to 192.168.187.128 \]](#)

2.1.19 Medium 22/tcp

Medium (CVSS: 5.3)

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

Summary

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

Quality of Detection (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.

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

- ephemeraly generated key exchange groups uses SHA-1

- using RSA 1024-bit modulus key

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

... continues on next page ...

| |
|---|
| ...continued from previous page ... |
| OID:1.3.6.1.4.1.25623.1.0.150713 Version used: 2024-06-14T05:05:48Z |
| 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) |
| Summary The remote SSH server is configured to allow / support weak host key algorithm(s). |
| Quality of Detection (QoD): 80% |
| Vulnerability Detection Result The remote SSH server supports the following weak host key algorithm(s): host key algorithm Description ----- ssh-dss Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS) |
| Solution: Solution type: Mitigation Disable the reported weak host key algorithm(s). |
| Vulnerability Detection Method Checks the supported host key algorithms of the remote SSH server. Currently weak host key algorithms are defined as the following: - ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS) Details: Weak Host Key Algorithm(s) (SSH) OID:1.3.6.1.4.1.25623.1.0.117687 Version used: 2024-06-14T05:05:48Z |
| References url: https://www.rfc-editor.org/rfc/rfc8332 url: https://www.rfc-editor.org/rfc/rfc8709 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6 |

| |
|---|
| Medium (CVSS: 4.3) |
| NVT: Weak Encryption Algorithm(s) Supported (SSH) |
| Summary The remote SSH server is configured to allow / support weak encryption algorithm(s). |
| Quality of Detection (QoD): 80% |
| Vulnerability Detection Result 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 |
| Solution: Solution type: Mitigation Disable the reported weak encryption algorithm(s). |
| Vulnerability Insight - The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore. - The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it. |
| ... 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. |
| Vulnerability Detection Method Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak encryption algorithms are defined as the following: <ul style="list-style-type: none"> - 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: 2024-06-14T05:05:48Z |
| References url: https://www.rfc-editor.org/rfc/rfc8758 url: https://www.kb.cert.org/vuls/id/958563 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3 |

[[return to 192.168.187.128](#)]

2.1.20 Low 25/tcp

| |
|---|
| Low (CVSS: 3.7) |
| NVT: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam) |
| Summary This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack. |
| Quality of Detection (QoD): 80% |
| 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 |
| ... continues on next page ... |

| |
|---|
| ...continued from previous page ... |
| 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 - If running OpenSSL update to version 1.0.2b or 1.0.1n or later. |
| Affected Software/OS - Hosts accepting 'DHE_EXPORT' cipher suites - OpenSSL version before 1.0.2b and 1.0.1n |
| Vulnerability Insight Flaw is triggered when handling Diffie-Hellman key exchanges defined in the 'DHE_EXPORT' cipher suites. |
| Vulnerability Detection Method Check previous collected cipher suites saved in the KB. Details: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam) OID:1.3.6.1.4.1.25623.1.0.805188 Version used: 2024-09-30T08:38:05Z |
| References cve: CVE-2015-4000 url: https://weakdh.org url: http://www.securityfocus.com/bid/74733 url: https://weakdh.org/imperfect-forward-secrecy.pdf url: http://openwall.com/lists/oss-security/2015/05/20/8 url: https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained url: https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes 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 |
| ... continues on next page ... |

...continued from previous page ...

cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0964
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
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

...continues on next page ...

| |
|-------------------------------------|
| ...continued from previous page ... |
| 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) |
| 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 |
| References cve: CVE-2014-3566 url: https://www.openssl.org/~bodo/ssl-poodle.pdf |
| ... continues on next page ... |

...continued from previous page...

```

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
    ↪g-ssl-30.html
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

```

[\[return to 192.168.187.128 \]](#)

2.1.21 Low 5432/tcp

Low (CVSS: 3.4)

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

Summary

This host is prone to an information disclosure vulnerability.

... continues on next page ...

| |
|---|
| ...continued from previous page ... |
| 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 |
| 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-↪g-ssl-30.html 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
```

[\[return to 192.168.187.128 \]](#)

2.1.22 Low 22/tcp

Low (CVSS: 2.6)

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

Summary

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

Quality of Detection (QoD): 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

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

umac-64@openssh.com

Solution:

... continues on next page ...

...continued from previous page ...

Solution type: Mitigation

Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method

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

Currently weak MAC algorithms are defined as the following:

- 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

References

url: <https://www.rfc-editor.org/rfc/rfc6668>

url: <https://www.rfc-editor.org/rfc/rfc4253#section-6.4>

[\[return to 192.168.187.128 \]](#)

This file was automatically generated.