Scan Report

April 7, 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 "DokuWiki Scan". The scan started at Sun Mar 31 23:01:04 2024 UTC and ended at Mon Apr 1 03:22:47 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
172.16.36.133	13	10	2	0	0
Total: 1	13	10	2	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 25 results selected by the filtering described above. Before filtering there were 140 results.

2 Results per Host

2.1 172.16.36.133

Host scan start	Sun Mar 31 23:02:30 2024 UTC
Host scan end	Mon Apr 1 03:22:43 2024 UTC

Service (Port)	Threat Level
443/tcp	High
80/tcp	High
12321/tcp	High
general/tcp	High
443/tcp	Medium
22/tcp	Medium
12320/tcp	Medium
12321/tcp	Medium
general/icmp	Low
22/tcp	Low

2.1.1 High 443/tcp

High (CVSS: 8.6)

NVT: DokuWiki Reflected File Download Vulnerability

Summary
The call parameter of /lib/exe/ajax.php in DokuWiki does not properly encode user input, which leads to a reflected file download vulnerability, and allows remote attackers to run arbitrary programs.

Quality of Detection: 99

Vulnerability Detection Result

```
Vulnerable URL: https://172.16.36.133/lib/exe/ajax.php?call=%7c%7c%63%61%6c%63%7
↪c%7c
```

Solution:
Solution type: VendorFix
Apply the provided patch.

Affected Software/OS
DokuWiki 2017-02-19e and prior.

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `DokuWiki Reflected File Download Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.140814
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2017-18123
url: https://github.com/splitbrain/dokuwiki/issues/2029
dfn-cert: DFN-CERT-2018-1733
dfn-cert: DFN-CERT-2018-1317
```

[return to 172.16.36.133]

2.1.2 High 80/tcp

High (CVSS: 8.6)

NVT: DokuWiki Reflected File Download Vulnerability

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The call parameter of /lib/exe/ajax.php in DokuWiki does not properly encode user input, which leads to a reflected file download vulnerability, and allows remote attackers to run arbitrary programs.

Quality of Detection: 99

Vulnerability Detection Result

```
Vulnerable URL: http://172.16.36.133/lib/exe/ajax.php?call=%7c%7c%63%61%6c%63%7c
↪%7c
```

Solution:
Solution type: VendorFix
Apply the provided patch.

Affected Software/OS
DokuWiki 2017-02-19e and prior.

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `DokuWiki Reflected File Download Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.140814
Version used: `2023-07-20T05:05:17Z`

References

```
cve: CVE-2017-18123
url: https://github.com/splitbrain/dokuwiki/issues/2029
dfn-cert: DFN-CERT-2018-1733
dfn-cert: DFN-CERT-2018-1317
```

[return to 172.16.36.133]

2.1.3 High 12321/tcp

High (CVSS: 9.8)

NVT: Webmin < 1.997 XSS Vulnerability

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

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 1.831
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     1.997
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 1.997 or later.

Affected Software/OS
Webmin version prior to 1.997.

Vulnerability Insight
Software/apt-lib.pl in Webmin lacks HTML escaping for a UI command.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Webmin < 1.997 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.124131
Version used: `2023-10-19T05:05:21Z`

References

```
cve: CVE-2022-36446
url: https://www.webmin.com/security.html
url: https://github.com/webmin/webmin/commit/13f7bf9621a82d93f1e9dbd838d1e220202
↪21bde
cert-bund: WID-SEC-2022-0825
```

High (CVSS: 9.8)

NVT: Webmin 1.880 Information Disclosure Vulnerability

Summary
Webmin is prone to an information disclosure vulnerability that allows non-privileged users to access arbitrary files.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 1.831
Fixed version:     Please see the solution tag for an available Mitigation
```

Impact
Successful exploitation would allow an attacker to access any file on the system, ranging from sensitive documents to administrator passwords.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: Mitigation
No patch is available as of 15th March, 2018. As a mitigation technique, the setting 'Can view any file as a log file' can be disabled, effectively stopping a user from exploiting this vulnerability.

Affected Software/OS
Webmin through version 1.880

Vulnerability Insight
An issue was discovered in Webmin when the default Yes setting of 'Can view any file as a log file' is enabled. As a result of weak default configuration settings, limited users have full access rights to the underlying Unix system files, allowing the user to read sensitive data from the local system (using Local File Include) such as the '/etc/shadow' file via a 'GET /syslog/save_log.cgi?view=1&file=/etc/shadow' request.

Vulnerability Detection Method
The script checks if a vulnerable version is present on the target host.
Details: `Webmin 1.880 Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113135
Version used: `2023-07-20T05:05:18Z`

References

```
cve: CVE-2018-8712
url: https://www.7elements.co.uk/resources/technical-advisories/webmin-1-840-1-8
↪80-unrestricted-access-arbitrary-files-using-local-file-include/
url: http://www.webmin.com/changes.html
```

High (CVSS: 9.6)

NVT: Webmin <= 1.994 Multiple Vulnerabilities

Summary
Webmin is prone to multiple vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 1.831
Fixed version:     None
Installation
path / port:       /
```

Solution:
Solution type: WillNotFix

. . . continues on next page . . .

. . . continued from previous page . . .

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
Webmin version 1.994 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2021-32156: A cross-site request forgery (CSRF) vulnerability exists via the Scheduled Cron Jobs feature.
- CVE-2021-32157: A cross-site scripting (XSS) vulnerability exists via the Scheduled Cron Jobs feature.
- CVE-2021-32158: An XSS vulnerability exists via the Upload and Download feature.
- CVE-2021-32159: A CSRF vulnerability exists via the Upload and Download feature.
- CVE-2021-32160: An XSS vulnerability exists through the Add Users feature.
- CVE-2021-32161: An XSS vulnerability exists through the File Manager feature.
- CVE-2021-32162: A CSRF vulnerability exists through the File Manager feature.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Webmin <= 1.994 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.127047
Version used: `2023-10-19T05:05:21Z`

References
```
cve: CVE-2021-32156
cve: CVE-2021-32157
cve: CVE-2021-32158
cve: CVE-2021-32159
cve: CVE-2021-32160
cve: CVE-2021-32161
cve: CVE-2021-32162
url: https://github.com/Mesh3l911/CVE-2021-32157
url: https://github.com/Mesh3l911/CVE-2021-32158
url: https://github.com/Mesh3l911/CVE-2021-32159
url: https://github.com/Mesh3l911/CVE-2021-32160
url: https://github.com/Mesh3l911/CVE-2021-32161
url: https://github.com/Mesh3l911/CVE-2021-32162
cert-bund: CB-K22/0412
```

High (CVSS: 8.8)

NVT: Webmin <= 1.991 Privilege Escalation Vulnerability

Summary
Webmin is prone to a privilege escalation vulnerability.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 1.831
Fixed version:     1.994
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 1.994 or later.

Affected Software/OS
Webmin version 1.991 and prior.

Vulnerability Insight
Webmin, when the Authentic theme is used, allows remote code execution when a user has been manually created (i.e., not created in Virtualmin or Cloudmin). This occurs because settings-editor_write.cgi does not properly restrict the file parameter.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Webmin <= 1.991 Privilege Escalation Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.127014
Version used: `2022-05-26T03:04:21Z`

References

```
cve: CVE-2022-30708
url: https://github.com/esp0xdeadbeef/rce_webmin
url: https://github.com/webmin/webmin/issues/1635
url: https://www.webmin.com/security.html
cert-bund: CB-K22/0609
```

High (CVSS: 8.8)

NVT: Webmin <= 1.983 RCE Vulnerability

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Webmin is prone to a remote code execution (RCE) vulnerability.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 1.831
Fixed version:     None
Installation
path / port:       /
```

Solution:

Solution type: WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS

Webmin version 1.983 and prior.

Vulnerability Insight

Arbitrary command execution can occur in Webmin. Any user authorized for the Package Updates module can execute arbitrary commands with root privileges via vectors involving %0A and %0C.

NOTE: this issue exists because of an incomplete fix for CVE-2019-12840.

Vulnerability Detection Method

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

Details: `Webmin <= 1.983 RCE Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.145090

Version used: `2021-12-23T08:45:36Z`

References

```
cve: CVE-2020-35606
url: https://www.pentest.com.tr/exploits/Webmin-1962-PU-Escape-Bypass-Remote-Com
↪mand-Execution.html
```

High (CVSS: 8.8)

NVT: Webmin < 1.930 Remote Code Execution (RCE) Vulnerability

Summary

Webmin is prone to an authenticated remote code execution (RCE) vulnerability.

Quality of Detection: 80

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.831
Fixed version:     1.930
Installation
path / port:       /
```

Impact

Successful exploitation would allow an authenticated attacker to gain control over the target system.

Solution:

Solution type: VendorFix

Update to version 1.930 or later.

Affected Software/OS

Webmin version 1.920 and prior.

Vulnerability Insight

rpc.cgi in Webmin through 1.920 allows authenticated Remote Code Execution via a crafted object name because unserialise_variable makes an eval call.

Vulnerability Detection Method

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

Details: `Webmin < 1.930 Remote Code Execution (RCE) Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.142804

Version used: `2021-09-08T08:01:40Z`

References

```
cve: CVE-2019-15642
url: https://www.calypt.com/blog/index.php/authenticated-rce-on-webmin/
url: https://github.com/webmin/webmin/commit/df8a43fb4bdc9c858874f72773bcba597ae
↪9432c
cert-bund: CB-K19/0786
```

High (CVSS: 8.8)

NVT: Webmin <= 1.941 Remote Code Execution (RCE) Vulnerability

Summary

Webmin is prone to a remote code execution (RCE) vulnerability.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 1.831
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     None
Installation
path / port:       /
```

Impact

Successful exploitation would allow an authorized attacker to gain control over the target system.

Solution:

Solution type: WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS

Webmin through version 1.941.

Vulnerability Insight

Any user authorized to the 'Package Updates' module can execute arbitrary commands with root privileges via the data parameter to update.cgi.

Vulnerability Detection Method

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

Details: `Webmin <= 1.941 Remote Code Execution (RCE) Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.113409

Version used: `2021-09-08T08:01:40Z`

References

```
cve: CVE-2019-12840
url: https://pentest.com.tr/exploits/Webmin-1910-Package-Updates-Remote-Command-
↪Execution.html
url: https://www.exploit-db.com/exploits/46984
```

High (CVSS: 8.8)

NVT: Webmin <= 1.984 Multiple Vulnerabilities

Summary

Webmin is prone to multiple vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 1.831
Fixed version:     1.990
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:        /
```

Solution:
Solution type: VendorFix
Update to version 1.990 or later.

Affected Software/OS
Webmin version 1.984 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2022-0824: Improper access control leads to remote code execution (RCE)
- CVE-2022-0829: Improper authorization

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Webmin <= 1.984 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.147747
Version used: `2022-04-27T08:53:35Z`

References

```
cve: CVE-2022-0824
cve: CVE-2022-0829
url: https://www.webmin.com/security.html
url: https://huntr.dev/bounties/d0049a96-de90-4b1a-9111-94de1044f295/
url: https://huntr.dev/bounties/f2d0389f-d7d1-4f34-9f9d-268b0a0da05e/
url: https://github.com/webmin/webmin/commit/eeeea3c097f5cc473770119f7ac61f1dcfa
↪671b9
url: https://github.com/webmin/webmin/commit/39ea464f0c40b325decd6a5bfb7833fa4a1
↪42e38
cert-bund: CB-K22/0267
```

High (CVSS: 8.8)

NVT: Webmin <= 1.930 XXE Vulnerability

Summary
Webmin is prone to an authenticated XXE vulnerability in xmlrpc.cgi.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 1.831
Fixed version:     None
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:        /
```

Impact

Successful exploitation would allow an authenticated attacker to gain control over the target system.

Solution:

Solution type: WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS

Webmin version 1.930 and prior.

Vulnerability Detection Method

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

Details: `Webmin <= 1.930 XXE Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.142805

Version used: `2021-09-08T08:01:40Z`

References

```
cve: CVE-2019-15642
url: https://www.calypt.com/blog/index.php/authenticated-xxe-on-webmin/
cert-bund: CB-K19/0786
```

High (CVSS: 7.8)

NVT: Webmin <= 1.941 RCE Vulnerability

Summary

Webmin is prone to an authenticated remote code execution vulnerability.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 1.831
Fixed version:     None
```

Solution:

Solution type: WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Webmin through version 1.941. The vendor does not classify this vulnerability as workable exploit, as it requires that the attacker already knows the root password. Hence there is no fix for it in Webmin.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Webmin <= 1.941 RCE Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141897
Version used: `2021-09-08T08:01:40Z`

References
```
cve: CVE-2019-9624
url: https://www.exploit-db.com/exploits/46201
url: http://www.webmin.com/security.html
```

[return to 172.16.36.133]

2.1.4 High general/tcp

High (CVSS: 10.0)

NVT: Operating System (OS) End of Life (EOL) Detection

Product detection result
```
cpe:/o:debian:debian_linux:8
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)
```

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: 80

Vulnerability Detection Result
```
The "Debian GNU/Linux" Operating System on the remote host has reached the end o
↪f life.
CPE:               cpe:/o:debian:debian_linux:8
Installed version,
build or SP:       8
EOL date:          2020-06-30
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
EOL info:          https://en.wikipedia.org/wiki/List_of_Debian_releases#Release
↪_table
```

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`

Product Detection Result

Product: `cpe:/o:debian:debian_linux:8`

Method: `OS Detection Consolidation and Reporting`

OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 172.16.36.133]

2.1.5 Medium 443/tcp

Medium (CVSS: 4.3)

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

Summary

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

Quality of Detection: 98

Vulnerability Detection Result

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

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

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

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

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2023-10-20T16:09:12Z`

References
```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
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
```

. . . 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: 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 Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2023-07-21T05:05:22Z`

References
`url: https://weakdh.org/`
`url: https://weakdh.org/sysadmin.html`

[return to 172.16.36.133]

2.1.6 Medium 22/tcp

Medium (CVSS: 5.3)

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

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

Quality of Detection: 80

Vulnerability Detection Result

```
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
--------------------------------------------------------------------------------
↪---------
ssh-dss            | Digital Signature Algorithm (DSA) / Digital Signature Stand
↪ard (DSS)
```

Solution:
Solution type: Mitigation
Disable the reported weak host key algorithm(s).

Vulnerability Detection Method
Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: `Weak Host Key Algorithm(s) (SSH)`
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: `2023-10-12T05:05:32Z`

References
```
url: https://www.rfc-editor.org/rfc/rfc8332
url: https://www.rfc-editor.org/rfc/rfc8709
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6
```

[return to 172.16.36.133]

2.1.7 Medium 12320/tcp

Medium (CVSS: 4.3)

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

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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

Quality of Detection: 98

Vulnerability Detection Result

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

Impact

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

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

Solution:

Solution type: Mitigation

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

Affected Software/OS

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

Vulnerability Insight

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:

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

Vulnerability Detection Method

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

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

OID:1.3.6.1.4.1.25623.1.0.117274

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

References

```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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: 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 Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2023-07-21T05:05:22Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html
```

[return to 172.16.36.133]

2.1.8 Medium 12321/tcp

Medium (CVSS: 6.1)

NVT: Webmin < 2.003 XSS Vulnerability

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

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 1.831
Fixed version:     2.003
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 2.003 or later.
Note: While there is no dedicated mention of the fix in any changelog the relevant code fix/commit as been included in the GitHub tag '2.003'.

Affected Software/OS
Webmin prior to version 2.003.

Vulnerability Insight
An XSS vulnerability exists in an unknown function of the file xterm/index.cgi.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Webmin < 2.003 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.126206
Version used: `2023-11-10T16:09:31Z`

References

```
cve: CVE-2022-3844
url: https://github.com/webmin/webmin/compare/2.001...2.003
url: https://github.com/webmin/webmin/commit/d3d33af3c0c3fd3a889c84e287a038b7a45
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪7d811
cert-bund: WID-SEC-2022-1957
```

Medium (CVSS: 6.1)

NVT: Webmin <= 1.941 Multiple XSS Vulnerabilities

Summary
Webmin is prone to multiple cross-site scripting vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 1.831
Fixed version:     1.953
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 1.953 or later.

Affected Software/OS
Webmin version 1.941 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- XSS in the Command Shell module (CVE-2020-8820 and CVE-2020-8821)
- XSS in the Read Mail module (CVE-2020-12670)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Webmin <= 1.941 Multiple XSS Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.144734
Version used: `2021-08-16T12:00:57Z`

References

```
cve: CVE-2020-8820
cve: CVE-2020-8821
cve: CVE-2020-12670
url: https://www.webmin.com/security.html
cert-bund: CB-K20/0973
```

Medium (CVSS: 6.1)

NVT: Webmin <= 1.995 XSS Vulnerability

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

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 1.831
Fixed version:     None
Installation
path / port:       /
```

Impact
An HTML email crafted by an attacker could capture browser cookies when opened.

Solution:
Solution type: WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
Webmin version 1.995 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Webmin <= 1.995 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.126099
Version used: `2023-08-03T05:05:16Z`

References

```
cve: CVE-2022-36880
url: https://www.webmin.com/security.html
cert-bund: WID-SEC-2022-0838
```

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.

. . . continues on next page . . .

. . . continued from previous page . . .

Quality of Detection: 98

Vulnerability Detection Result

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

Impact

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

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

Solution:

Solution type: Mitigation

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

Affected Software/OS

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

Vulnerability Insight

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:

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

Vulnerability Detection Method

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

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

OID:1.3.6.1.4.1.25623.1.0.117274

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

References

```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

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: 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 Vulnerabili.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.106223

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

References

```
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html
```

[return to 172.16.36.133]

2.1.9 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

Vulnerability Detection Result

```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References

```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 172.16.36.133]

2.1.10 Low 22/tcp

Low (CVSS: 2.6)

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

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

Solution:

Solution type: Mitigation

Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method

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

Currently weak MAC algorithms are defined as the following:

- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm

Details: `Weak MAC Algorithm(s) Supported (SSH)`

OID:1.3.6.1.4.1.25623.1.0.105610

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

References

```
url: https://www.rfc-editor.org/rfc/rfc6668
```

. . . continues on next page . . .

. . . continued from previous page . . .
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[return to 172.16.36.133]

This file was automatically generated.