

Scan Report

March 5, 2025

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “New Quick Task”. The scan started at Tue Mar 4 16:52:20 2025 UTC and ended at Tue Mar 4 21:49:51 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1	Result Overview	2
1.1	Host Authentications	2
2	Results per Host	3
2.1	10.0.0.245	3
2.1.1	High 443/tcp	3
2.1.2	Low general/icmp	3
2.1.3	Low general/tcp	4
2.2	10.0.0.92	6
2.2.1	High 80/tcp	6
2.2.2	High 3128/tcp	37
2.2.3	High general/tcp	57
2.2.4	High 22/tcp	197
2.2.5	High 53/tcp	204
2.2.6	Medium 80/tcp	206
2.2.7	Medium 3128/tcp	225
2.2.8	Medium 21/tcp	229
2.2.9	Medium general/tcp	229
2.2.10	Medium 22/tcp	390
2.2.11	Medium 25/tcp	404
2.2.12	Low general/tcp	405
2.2.13	Low 22/tcp	406

2.2.14	Low general/icmp	407
2.3	10.0.0.116	408
2.3.1	High 443/tcp	409
2.4	10.0.0.1	409
2.4.1	High 443/tcp	410
2.4.2	High 53/tcp	412
2.4.3	Medium 12865/tcp	417
2.4.4	Medium 443/tcp	417
2.4.5	Medium 53/tcp	427
2.4.6	Medium 80/tcp	429
2.4.7	Low general/icmp	437
2.4.8	Low general/tcp	438
2.5	10.0.0.176	440
2.5.1	Low general/tcp	440
2.6	10.0.0.175	441
2.6.1	Low general/tcp	441
2.6.2	Low general/icmp	442
2.7	10.0.0.190	443
2.7.1	Low general/icmp	444
2.8	10.0.0.141	445
2.8.1	Low general/icmp	445

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.0.0.245	1	0	2	0	0
10.0.0.92	132	132	3	0	0
10.0.0.116	1	0	0	0	0
10.0.0.1	4	13	2	0	0
10.0.0.176	0	0	1	0	0
10.0.0.175	0	0	2	0	0
10.0.0.190	0	0	1	0	0
10.0.0.141	0	0	1	0	0
Total: 8	138	145	12	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.

This report contains all 295 results selected by the filtering described above. Before filtering there were 550 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
10.0.0.245	SSH	Failure	Protocol SSH, Port 22, User student : Login failure
10.0.0.92	SSH	Success	Protocol SSH, Port 22, User student
10.0.0.92	SMB	Success	Protocol SMB, Port 445, User student
10.0.0.116	SSH	Failure	Protocol SSH, Port 22, User student : Login failure
10.0.0.1	SSH	Failure	Protocol SSH, Port 22, User student : Login failure
10.0.0.176	SSH	Failure	Protocol SSH, Port 22, User student : Login failure
10.0.0.175	SSH	Failure	Protocol SSH, Port 22, User student : Login failure
10.0.0.190	SSH	Failure	Protocol SSH, Port 22, User student : Login failure
10.0.0.141	SSH	Failure	Protocol SSH, Port 22, User student : Login failure

2 Results per Host

2.1 10.0.0.245

Host scan start Tue Mar 4 17:46:11 2025 UTC

Host scan end Tue Mar 4 19:17:18 2025 UTC

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

2.1.1 High 443/tcp

High (CVSS: 10.0) NVT: Greenbone Security Assistant (GSA) Default Credentials (HTTP)
Summary The remote Greenbone Security Assistant (GSA) is installed / configured in a way that it has account(s) with default passwords enabled.
Quality of Detection (QoD): 100%
Vulnerability Detection Result It was possible to login using the following credentials (username:password): admin:admin
Impact This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.
Solution: Solution type: Workaround Change the password of the mentioned account(s).
Vulnerability Detection Method Tries to login with known default credentials via the HTTP protocol. Details: Greenbone Security Assistant (GSA) Default Credentials (HTTP) OID:1.3.6.1.4.1.25623.1.0.105354 Version used: 2024-07-10T05:05:27Z

[\[return to 10.0.0.245 \]](#)

2.1.2 Low general/icmp

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

[\[return to 10.0.0.245 \]](#)

2.1.3 Low general/tcp

Low (CVSS: 2.6) NVT: TCP Timestamps Information Disclosure
Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.
Quality of Detection (QoD): 80%
Vulnerability Detection Result It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 382270235 Packet 2: 382271305
Impact A side effect of this feature is that the uptime of the remote host can sometimes be computed.
Solution: Solution type: Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
Affected Software/OS TCP implementations that implement RFC1323/RFC7323.
Vulnerability Insight The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
Vulnerability Detection Method Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
References url: https://datatracker.ietf.org/doc/html/rfc1323 url: https://datatracker.ietf.org/doc/html/rfc7323 url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152 url: https://www.fortiguard.com/psirt/FG-IR-16-090

[\[return to 10.0.0.245 \]](#)

2.2 10.0.0.92

Host scan start Tue Mar 4 16:54:18 2025 UTC
Host scan end Tue Mar 4 18:23:07 2025 UTC

Service (Port)	Threat Level
80/tcp	High
3128/tcp	High
general/tcp	High
22/tcp	High
53/tcp	High
80/tcp	Medium
3128/tcp	Medium
21/tcp	Medium
general/tcp	Medium
22/tcp	Medium
25/tcp	Medium
general/tcp	Low
22/tcp	Low
general/icmp	Low

2.2.1 High 80/tcp

High (CVSS: 10.0) NVT: PHP End of Life (EOL) Detection - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary The PHP version on the remote host has reached the end of life (EOL) and should not be used anymore.
Quality of Detection (QoD): 30%
Vulnerability Detection Result The "PHP" version on the remote host has reached the end of life. CPE: cpe:/a:php:php:7.2.34 Installed version: 7.2.34 EOL version: 7.2 EOL date: 2020-11-30
... continues on next page ...

...continued from previous page ...
Impact An EOL version of PHP is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.
Solution: Solution type: VendorFix Update the PHP version on the remote host to a still supported version.
Vulnerability Insight Each release branch of PHP is fully supported for two years from its initial stable release. During this period, bugs and security issues that have been reported are fixed and are released in regular point releases. After this two year period of active support, each branch is then supported for an additional year for critical security issues only. Releases during this period are made on an as-needed basis: there may be multiple point releases, or none, depending on the number of reports. Once the three years of support are completed, the branch reaches its end of life and is no longer supported.
Vulnerability Detection Method Checks if an EOL version is present on the target host. Details: PHP End of Life (EOL) Detection - Linux OID:1.3.6.1.4.1.25623.1.0.105889 Version used: 2024-02-28T14:37:42Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References url: https://secure.php.net/supported-versions.php url: https://secure.php.net/eol.php
High (CVSS: 9.8) NVT: PHP < 8.0.30, 8.1.x < 8.1.22, 8.2.x < 8.2.9 Security Update - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to multiple vulnerabilities.
... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 8.0.30 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 8.0.30, 8.1.22, 8.2.9 or later.
Affected Software/OS PHP prior to version 8.0.30, 8.1.x prior to 8.1.22 and 8.2.x prior to 8.2.9.
Vulnerability Insight The following flaws exist: - CVE-2023-3823: Fixed bug GHSA-3qrf-m4j2-pcrr (Security issue with external entity loading in XML without enabling it) - CVE-2023-3824: Fixed bug GHSA-jqcx-ccgc-xwhv (Buffer mismanagement in phar_dir_read())
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 8.0.30, 8.1.x < 8.1.22, 8.2.x < 8.2.9 Security Update - Linux OID:1.3.6.1.4.1.25623.1.0.170529 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2023-3823 cve: CVE-2023-3824 url: https://www.php.net/ChangeLog-8.php#8.1.22 url: https://www.php.net/ChangeLog-8.php#8.0.30 url: https://www.php.net/ChangeLog-8.php#8.2.9 url: https://github.com/php/php-src/security/advisories/GHSA-3qrf-m4j2-pcrr url: https://github.com/php/php-src/security/advisories/GHSA-jqcx-ccgc-xwhv cert-bund: WID-SEC-2023-2917 cert-bund: WID-SEC-2023-2679 cert-bund: WID-SEC-2023-1970 dfn-cert: DFN-CERT-2024-3330
... continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2024-2681 dfn-cert: DFN-CERT-2024-0993 dfn-cert: DFN-CERT-2023-2570 dfn-cert: DFN-CERT-2023-2542 dfn-cert: DFN-CERT-2023-1775
High (CVSS: 9.8) NVT: PHP < 7.4.33, 8.0.x < 8.0.25, 8.1.x < 8.1.12 Security Update - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.4.33 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 7.4.33, 8.0.25, 8.1.12 or later.
Affected Software/OS PHP prior to version 7.4.33, version 8.0.x through 8.0.24 and 8.1.x through 8.1.11.
Vulnerability Insight The following vulnerabilities exist: - CVE-2022-31630: OOB read due to insufficient input validation in imageloadfont() - CVE-2022-37454: Buffer overflow in hash_update() on long parameter
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.4.33, 8.0.x < 8.0.25, 8.1.x < 8.1.12 Security Update - Linux OID:1.3.6.1.4.1.25623.1.0.148830 Version used: 2023-10-19T05:05:21Z
Product Detection Result Product: cpe:/a:php:php:7.2.34
... continues on next page ...

...continued from previous page ...	
Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)	
References cve: CVE-2022-31630 cve: CVE-2022-37454 url: https://www.php.net/ChangeLog-7.php#7.4.33 url: https://www.php.net/ChangeLog-8.php#8.0.25 url: https://www.php.net/ChangeLog-8.php#8.1.12 cert-bund: WID-SEC-2023-1021 cert-bund: WID-SEC-2023-0561 cert-bund: WID-SEC-2023-0138 cert-bund: WID-SEC-2022-1934 cert-bund: WID-SEC-2022-1816 dfn-cert: DFN-CERT-2023-0552 dfn-cert: DFN-CERT-2023-0422 dfn-cert: DFN-CERT-2023-0028 dfn-cert: DFN-CERT-2022-2869 dfn-cert: DFN-CERT-2022-2793 dfn-cert: DFN-CERT-2022-2715 dfn-cert: DFN-CERT-2022-2639 dfn-cert: DFN-CERT-2022-2638 dfn-cert: DFN-CERT-2022-2598 dfn-cert: DFN-CERT-2022-2535 dfn-cert: DFN-CERT-2022-2523 dfn-cert: DFN-CERT-2022-2420 dfn-cert: DFN-CERT-2022-2380	
High (CVSS: 9.8) NVT: PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Linux	
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)	
Summary PHP released new versions which include a security fix.	
Quality of Detection (QoD): 30%	
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.4.28 Installation	
... continues on next page ...	

...continued from previous page...	
path / port:	80/tcp
Solution: Solution type: VendorFix Update to version 7.4.28, 8.0.16, 8.1.3 or later.	
Affected Software/OS PHP prior to version 7.4.28, 8.0.x through 8.0.15 and 8.1.x through 8.1.2.	
Vulnerability Insight Fix #81708: UAF due to <code>php_filter_float()</code> failing for ints.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Linux OID:1.3.6.1.4.1.25623.1.0.147657 Version used: 2022-03-09T03:03:43Z	
Product Detection Result Product: <code>cpe:/a:php:php:7.2.34</code> Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)	
References cve: CVE-2021-21708 url: https://www.php.net/ChangeLog-7.php#7.4.28 url: https://www.php.net/ChangeLog-8.php#8.0.16 url: https://www.php.net/ChangeLog-8.php#8.1.3 url: https://bugs.php.net/bug.php?id=81708 cert-bund: WID-SEC-2023-1737 cert-bund: WID-SEC-2022-1767 cert-bund: WID-SEC-2022-1335 cert-bund: WID-SEC-2022-1228 cert-bund: WID-SEC-2022-0280 cert-bund: CB-K22/0201 dfn-cert: DFN-CERT-2024-1062 dfn-cert: DFN-CERT-2023-1600 dfn-cert: DFN-CERT-2022-2639 dfn-cert: DFN-CERT-2022-2598 dfn-cert: DFN-CERT-2022-2500 dfn-cert: DFN-CERT-2022-2499 dfn-cert: DFN-CERT-2022-1605 dfn-cert: DFN-CERT-2022-0557 dfn-cert: DFN-CERT-2022-0407 dfn-cert: DFN-CERT-2022-0365	

High (CVSS: 9.8) NVT: Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux
Product detection result cpe:/a:apache:http_server:2.4.52 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.117232)
Summary Apache HTTP Server is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 2.4.52 Fixed version: 2.4.53 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 2.4.53 or later.
Affected Software/OS Apache HTTP Server version 2.4.52 and prior.
Vulnerability Insight The following vulnerabilities exist: - CVE-2022-22719: mod_lua Use of uninitialized value of in r:parsebody - CVE-2022-22720: HTTP request smuggling vulnerability - CVE-2022-22721: Possible buffer overflow with very large or unlimited LimitXMLRequestBody - CVE-2022-23943: mod_sed: Read/write beyond bounds
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux OID:1.3.6.1.4.1.25623.1.0.113837 Version used: 2022-03-21T03:03:41Z
Product Detection Result Product: cpe:/a:apache:http_server:2.4.52 Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)
References ... continues on next page ...

...continued from previous page ...

url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.53

cve: CVE-2022-22719

cve: CVE-2022-22720

cve: CVE-2022-22721

cve: CVE-2022-23943

cert-bund: WID-SEC-2024-1591

cert-bund: WID-SEC-2022-1772

cert-bund: WID-SEC-2022-1335

cert-bund: WID-SEC-2022-1228

cert-bund: WID-SEC-2022-1161

cert-bund: WID-SEC-2022-1057

cert-bund: WID-SEC-2022-0898

cert-bund: WID-SEC-2022-0799

cert-bund: WID-SEC-2022-0755

cert-bund: WID-SEC-2022-0646

cert-bund: WID-SEC-2022-0432

cert-bund: WID-SEC-2022-0302

cert-bund: WID-SEC-2022-0290

cert-bund: CB-K22/0619

cert-bund: CB-K22/0306

dfn-cert: DFN-CERT-2022-2799

dfn-cert: DFN-CERT-2022-2509

dfn-cert: DFN-CERT-2022-2305

dfn-cert: DFN-CERT-2022-2167

dfn-cert: DFN-CERT-2022-1116

dfn-cert: DFN-CERT-2022-1115

dfn-cert: DFN-CERT-2022-1114

dfn-cert: DFN-CERT-2022-0899

dfn-cert: DFN-CERT-2022-0898

dfn-cert: DFN-CERT-2022-0865

dfn-cert: DFN-CERT-2022-0747

dfn-cert: DFN-CERT-2022-0678

dfn-cert: DFN-CERT-2022-0582

High (CVSS: 9.8)

NVT: Apache HTTP Server < 2.4.60 Multiple Vulnerabilities - Linux

Product detection result

cpe:/a:apache:http_server:2.4.52

Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)**Summary**

Apache HTTP Server is prone to multiple vulnerabilities.

... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 2.4.52 Fixed version: 2.4.60 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 2.4.60 or later.
Affected Software/OS Apache HTTP Server version 2.4.59 and prior.
Vulnerability Insight The following flaws exist: - CVE-2024-36387: Denial of Service (DoS) by Null pointer in websocket over HTTP/2 - CVE-2024-38473: Proxy encoding problem - CVE-2024-38474: Weakness with encoded question marks in backreferences - CVE-2024-38475: Weakness in mod_rewrite when first segment of substitution matches filesystem path - CVE-2024-38476: May use exploitable/malicious backend application output to run local handlers via internal redirect - CVE-2024-38477: Crash resulting in DoS in mod_proxy via a malicious request - CVE-2024-39573: mod_rewrite proxy handler substitution
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server < 2.4.60 Multiple Vulnerabilities - Linux OID:1.3.6.1.4.1.25623.1.0.114682 Version used: 2024-08-22T05:05:50Z
Product Detection Result Product: cpe:/a:apache:http_server:2.4.52 Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)
References cve: CVE-2024-36387 cve: CVE-2024-38473 cve: CVE-2024-38474 cve: CVE-2024-38475 cve: CVE-2024-38476 cve: CVE-2024-38477
... continues on next page ...

...continued from previous page ...
<div>cve: CVE-2024-39573 url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.60 cert-bund: WID-SEC-2025-0148 cert-bund: WID-SEC-2025-0143 cert-bund: WID-SEC-2024-3291 cert-bund: WID-SEC-2024-3199 cert-bund: WID-SEC-2024-1913 cert-bund: WID-SEC-2024-1504 dfn-cert: DFN-CERT-2025-0170 dfn-cert: DFN-CERT-2024-2841 dfn-cert: DFN-CERT-2024-2787 dfn-cert: DFN-CERT-2024-2736 dfn-cert: DFN-CERT-2024-2342 dfn-cert: DFN-CERT-2024-2214 dfn-cert: DFN-CERT-2024-2201 dfn-cert: DFN-CERT-2024-2180 dfn-cert: DFN-CERT-2024-2110 dfn-cert: DFN-CERT-2024-2017 dfn-cert: DFN-CERT-2024-1963 dfn-cert: DFN-CERT-2024-1920 dfn-cert: DFN-CERT-2024-1919 dfn-cert: DFN-CERT-2024-1911 dfn-cert: DFN-CERT-2024-1907 dfn-cert: DFN-CERT-2024-1893 dfn-cert: DFN-CERT-2024-1816 dfn-cert: DFN-CERT-2024-1811 dfn-cert: DFN-CERT-2024-1784 dfn-cert: DFN-CERT-2024-1741 dfn-cert: DFN-CERT-2024-1699</div>

<div>High (CVSS: 9.8) NVT: Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Linux</div>
<div>Product detection result cpe:/a:apache:http_server:2.4.52 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1 ↪.0.117232)</div>
<div>Summary Apache HTTP Server is prone to multiple vulnerabilities.</div>
<div>Quality of Detection (QoD): 30%</div>
<div>Vulnerability Detection Result Installed version: 2.4.52 Fixed version: 2.4.54</div>
<div>... continues on next page ...</div>

...continued from previous page...	
Installation	
path / port:	80/tcp
Solution:	
Solution type: VendorFix	
Update to version 2.4.54 or later.	
Affected Software/OS	
Apache HTTP Server version 2.4.53 and prior.	
Vulnerability Insight	
The following vulnerabilities exist:	
- CVE-2022-26377: mod_proxy_ajp: Possible request smuggling	
- CVE-2022-28614: Read beyond bounds via ap_rwrite()	
- CVE-2022-28615: Read beyond bounds in ap_stremp_match()	
- CVE-2022-29404: Denial of service in mod_lua r:parsebody	
- CVE-2022-30556: Information disclosure in mod_lua with websockets	
- CVE-2022-31813: mod_proxy X-Forwarded-For dropped by hop-by-hop mechanism	
Vulnerability Detection Method	
Checks if a vulnerable version is present on the target host.	
Details: Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Linux	
OID:1.3.6.1.4.1.25623.1.0.148252	
Version used: 2022-06-20T03:04:15Z	
Product Detection Result	
Product: cpe:/a:apache:http_server:2.4.52	
Method: Apache HTTP Server Detection Consolidation	
OID: 1.3.6.1.4.1.25623.1.0.117232)	
References	
cve: CVE-2022-26377	
cve: CVE-2022-28614	
cve: CVE-2022-28615	
cve: CVE-2022-29404	
cve: CVE-2022-30556	
cve: CVE-2022-31813	
url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.54	
cert-bund: WID-SEC-2024-1591	
cert-bund: WID-SEC-2023-1969	
cert-bund: WID-SEC-2023-0134	
cert-bund: WID-SEC-2023-0132	
cert-bund: WID-SEC-2022-1767	
cert-bund: WID-SEC-2022-1766	
cert-bund: WID-SEC-2022-1764	
...continues on next page...	

...continued from previous page ...
cert-bund: WID-SEC-2022-0858
cert-bund: WID-SEC-2022-0192
cert-bund: CB-K22/0692
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2789
dfn-cert: DFN-CERT-2022-2652
dfn-cert: DFN-CERT-2022-2509
dfn-cert: DFN-CERT-2022-2310
dfn-cert: DFN-CERT-2022-2167
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1833
dfn-cert: DFN-CERT-2022-1720
dfn-cert: DFN-CERT-2022-1353
dfn-cert: DFN-CERT-2022-1296

High (CVSS: 9.8) NVT: Apache HTTP Server 2.4.0 - 2.4.55 HTTP Request Smuggling Vulnerability - Linux
Product detection result cpe:/a:apache:http_server:2.4.52 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1 ↔.0.117232)
Summary Apache HTTP Server is prone to a HTTP request smuggling vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 2.4.52 Fixed version: 2.4.56 Installation path / port: 80/tcp
Impact Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning.
Solution: Solution type: VendorFix Update to version 2.4.56 or later.
Affected Software/OS
... continues on next page ...

...continued from previous page ...	
Apache HTTP Server versions 2.4.0 through 2.4.55.	
Vulnerability Insight Some mod_proxy configurations allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server 2.4.0 - 2.4.55 HTTP Request Smuggling Vulnerability - Linux OID:1.3.6.1.4.1.25623.1.0.104597 Version used: 2024-02-15T05:05:40Z	
Product Detection Result Product: cpe:/a:apache:http_server:2.4.52 Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)	
References cve: CVE-2023-25690 url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.56 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2023-3129 cert-bund: WID-SEC-2023-2694 cert-bund: WID-SEC-2023-2031 cert-bund: WID-SEC-2023-1809 cert-bund: WID-SEC-2023-1807 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-1021 cert-bund: WID-SEC-2023-0657 cert-bund: WID-SEC-2023-0583 dfn-cert: DFN-CERT-2023-1648 dfn-cert: DFN-CERT-2023-1297 dfn-cert: DFN-CERT-2023-1232 dfn-cert: DFN-CERT-2023-0884 dfn-cert: DFN-CERT-2023-0788 dfn-cert: DFN-CERT-2023-0658 dfn-cert: DFN-CERT-2023-0546	

High (CVSS: 9.8) NVT: PHP < 8.1.31, 8.2.x < 8.2.26, 8.3.x < 8.3.14 Multiple Vulnerabilities - Linux	
Product detection result	
... continues on next page ...	

...continued from previous page ...
cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 8.1.31 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 8.1.31, 8.2.26, 8.3.14 or later.
Affected Software/OS PHP versions prior to 8.1.31, 8.2.x prior to 8.2.26 and 8.3.x prior to 8.3.14.
Vulnerability Insight The following vulnerabilities exist: <ul style="list-style-type: none"> - CVE-2024-8929: Leak partial content of the heap through heap buffer over-read - CVE-2024-8932: OOB access in ldap_escape - CVE-2024-11233: Single byte overread with convert.quoted-printable-decode filter - CVE-2024-11234: Configuring a proxy in a stream context might allow for CRLF injection in URIs - CVE-2024-11236: Integer overflow in the firebird/dblib quoter causing OOB writes - No CVE: Heap-Use-After-Free in sapi_read_post_data Processing in CLI SAPI Interface
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 8.1.31, 8.2.x < 8.2.26, 8.3.x < 8.3.14 Multiple Vulnerabilities - Linux OID:1.3.6.1.4.1.25623.1.0.153495 Version used: 2025-01-13T08:32:03Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2024-8929
... continues on next page ...

...continued from previous page ...
cve: CVE-2024-8932
cve: CVE-2024-11233
cve: CVE-2024-11234
cve: CVE-2024-11236
url: https://www.php.net/ChangeLog-8.php#8.1.31
url: https://www.php.net/ChangeLog-8.php#8.2.26
url: https://www.php.net/ChangeLog-8.php#8.3.14
url: https://github.com/php/php-src/security/advisories/GHSA-h35g-vwh6-m678
url: https://github.com/php/php-src/security/advisories/GHSA-g665-fm4p-vhff
url: https://github.com/php/php-src/security/advisories/GHSA-r977-prxv-hc43
url: https://github.com/php/php-src/security/advisories/GHSA-c5f2-jwm7-mmq2
url: https://github.com/php/php-src/security/advisories/GHSA-5hqh-c84r-qjcv
url: https://github.com/php/php-src/security/advisories/GHSA-4w77-75f9-2c8w
cert-bund: WID-SEC-2024-3519
dfn-cert: DFN-CERT-2025-0179
dfn-cert: DFN-CERT-2024-3200
dfn-cert: DFN-CERT-2024-3172
dfn-cert: DFN-CERT-2024-3108

High (CVSS: 9.8) NVT: PHP < 8.1.29, 8.2.x < 8.2.20, 8.3.x < 8.3.8 Multiple Vulnerabilities - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 8.1.29 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 8.1.29, 8.2.20, 8.3.8 or later.
Affected Software/OS PHP prior to version 8.1.29, version 8.2.x through 8.2.19 and 8.3.x through 8.3.7.
Vulnerability Insight
... continues on next page ...

...continued from previous page...
<p>The following vulnerabilities exist:</p> <ul style="list-style-type: none"> - CVE-2024-4577: Argument injection in PHP-CGI (bypass of CVE-2012-1823) - CVE-2024-5458: Filter bypass in filter_var FILTER_VALIDATE_URL - CVE-2024-5585: Bypass of CVE-2024-1874 <p>Note: As of 06/2024 the CVEs CVE-2024-4577 and CVE-2024-5585 are known to be exploitable on Windows systems only.</p>
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: PHP < 8.1.29, 8.2.x < 8.2.20, 8.3.x < 8.3.8 Multiple Vulnerabilities - Linux</p> <p>OID:1.3.6.1.4.1.25623.1.0.152369</p> <p>Version used: 2024-08-09T05:05:42Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:php:php:7.2.34</p> <p>Method: PHP Detection (HTTP)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>References</p> <p>cve: CVE-2024-4577</p> <p>cve: CVE-2024-5458</p> <p>cve: CVE-2024-5585</p> <p>cisa: Known Exploited Vulnerability (KEV) catalog</p> <p>url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog</p> <p>url: https://www.php.net/ChangeLog-8.php#8.1.29</p> <p>url: https://www.php.net/ChangeLog-8.php#8.2.20</p> <p>url: https://www.php.net/ChangeLog-8.php#8.3.8</p> <p>url: https://github.com/php/php-src/security/advisories/GHSA-9fcc-425m-g385</p> <p>url: https://github.com/php/php-src/security/advisories/GHSA-w8qr-v226-r27w</p> <p>url: https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability-en/</p> <p>url: https://blog.orange.tw/2024/06/cve-2024-4577-yet-another-php-rce.html</p> <p>url: https://labs.watchtowr.com/no-way-php-strikes-again-cve-2024-4577/</p> <p>url: https://github.com/watchtowrlabs/CVE-2024-4577</p> <p>cert-bund: WID-SEC-2024-3196</p> <p>cert-bund: WID-SEC-2024-3195</p> <p>cert-bund: WID-SEC-2024-1320</p> <p>dfn-cert: DFN-CERT-2024-3330</p> <p>dfn-cert: DFN-CERT-2024-3329</p> <p>dfn-cert: DFN-CERT-2024-2707</p> <p>dfn-cert: DFN-CERT-2024-1853</p> <p>dfn-cert: DFN-CERT-2024-1586</p> <p>dfn-cert: DFN-CERT-2024-1574</p> <p>dfn-cert: DFN-CERT-2024-1563</p> <p>dfn-cert: DFN-CERT-2024-1476</p>

High (CVSS: 9.0) NVT: Apache HTTP Server < 2.4.55 Multiple Vulnerabilities - Linux
Product detection result cpe:/a:apache:http_server:2.4.52 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.117232)
Summary Apache HTTP Server is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 2.4.52 Fixed version: 2.4.55 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 2.4.55 or later.
Affected Software/OS Apache HTTP Server version 2.4.54 and prior.
Vulnerability Insight The following vulnerabilities exist: - CVE-2006-20001: mod_dav out of bounds read, or write of zero byte - CVE-2022-36760: Possible request smuggling in mod_proxy_ajp - CVE-2022-37436: mod_proxy allows a backend to trigger HTTP response splitting
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server < 2.4.55 Multiple Vulnerabilities - Linux OID:1.3.6.1.4.1.25623.1.0.149152 Version used: 2024-02-15T05:05:40Z
Product Detection Result Product: cpe:/a:apache:http_server:2.4.52 Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)
References cve: CVE-2006-20001
... continues on next page ...

...continued from previous page ...
cve: CVE-2022-36760 cve: CVE-2022-37436 url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.55 cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2023-2674 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-1022 cert-bund: WID-SEC-2023-0561 cert-bund: WID-SEC-2023-0110 dfn-cert: DFN-CERT-2023-2545 dfn-cert: DFN-CERT-2023-1895 dfn-cert: DFN-CERT-2023-1297 dfn-cert: DFN-CERT-2023-0658 dfn-cert: DFN-CERT-2023-0548 dfn-cert: DFN-CERT-2023-0497 dfn-cert: DFN-CERT-2023-0118

High (CVSS: 8.8)

NVT: PHP < 8.1.30, 8.2.x < 8.2.24, 8.3.x < 8.3.12 Multiple Vulnerabilities - Linux

Product detection result

cpe:/a:php:php:7.2.34

Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

PHP is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 7.2.34

Fixed version: 8.1.30

Installation

path / port: 80/tcp

Solution:

Solution type: VendorFix

Update to version 8.1.30, 8.2.24, 8.3.12 or later.

Affected Software/OS

PHP versions prior to 8.1.30, 8.2.x prior to 8.2.24 and 8.3.x prior to 8.3.12.

Vulnerability Insight

... continues on next page ...

...continued from previous page ...	
<p>The following vulnerabilities exist:</p> <ul style="list-style-type: none"> - CVE-2024-8925, CVE-2024-8928: Erroneous parsing of multipart form data - CVE-2024-8926: Bypass of CVE-2024-4577, Parameter Injection Vulnerability - CVE-2024-8927: cgi.force_redirect configuration is bypassable due to the environment variable collision - CVE-2024-9026: Logs from children may be altered 	
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 8.1.30, 8.2.x < 8.2.24, 8.3.x < 8.3.12 Multiple Vulnerabilities - Linux OID:1.3.6.1.4.1.25623.1.0.114787 Version used: 2024-10-17T08:02:35Z</p>	
<p>Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)</p>	
<p>References cve: CVE-2024-8925 cve: CVE-2024-8926 cve: CVE-2024-8927 cve: CVE-2024-8928 cve: CVE-2024-9026 url: https://www.php.net/ChangeLog-8.php#8.1.30 url: https://www.php.net/ChangeLog-8.php#8.2.24 url: https://www.php.net/ChangeLog-8.php#8.3.12 url: https://github.com/php/php-src/security/advisories/GHSA-9pqp-7h25-4f32 url: https://github.com/php/php-src/security/advisories/GHSA-p99j-rfp4-xqvq url: https://github.com/php/php-src/security/advisories/GHSA-94p6-54jq-9mwp url: https://github.com/php/php-src/security/advisories/GHSA-865w-9rf3-2wh5 url: https://bugzilla.redhat.com/show_bug.cgi?id=2317439 cert-bund: WID-SEC-2025-0137 cert-bund: WID-SEC-2024-3116 cert-bund: WID-SEC-2024-2230 dfn-cert: DFN-CERT-2025-0168 dfn-cert: DFN-CERT-2024-3330 dfn-cert: DFN-CERT-2024-3329 dfn-cert: DFN-CERT-2024-2707 dfn-cert: DFN-CERT-2024-2591 dfn-cert: DFN-CERT-2024-2550</p>	
<p>High (CVSS: 8.8) NVT: PHP < 7.4.30, 8.0.x < 8.0.20, 8.1.x < 8.1.7 Security Update (Jun 2022) - Linux</p>	
<p>Product detection result</p>	
... continues on next page ...	

...continued from previous page ...
cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP released new versions which include a security fix.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.4.30 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 7.4.30, 8.0.20, 8.1.7 or later.
Affected Software/OS PHP prior to version 7.4.30, 8.0.x through 8.0.19 and 8.1.x through 8.1.6.
Vulnerability Insight The following vulnerabilities exist: - CVE-2022-31625: Uninitialized array in pg_query_params() - CVE-2022-31626: mysqlnd/pdo password buffer overflow
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.4.30, 8.0.x < 8.0.20, 8.1.x < 8.1.7 Security Update (Jun 2022) - Linux OID:1.3.6.1.4.1.25623.1.0.148249 Version used: 2023-10-19T05:05:21Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2022-31625 cve: CVE-2022-31626 url: https://www.php.net/ChangeLog-7.php#7.4.30 url: https://www.php.net/ChangeLog-8.php#8.0.20 url: https://www.php.net/ChangeLog-8.php#8.1.7 url: https://bugs.php.net/bug.php?id=81720
... continues on next page ...

...continued from previous page ...
url: https://bugs.php.net/bug.php?id=81719 cert-bund: WID-SEC-2023-1737 cert-bund: WID-SEC-2022-0255 cert-bund: CB-K22/0700 dfn-cert: DFN-CERT-2023-1600 dfn-cert: DFN-CERT-2022-2869 dfn-cert: DFN-CERT-2022-2639 dfn-cert: DFN-CERT-2022-2638 dfn-cert: DFN-CERT-2022-2598 dfn-cert: DFN-CERT-2022-2500 dfn-cert: DFN-CERT-2022-2323 dfn-cert: DFN-CERT-2022-1881 dfn-cert: DFN-CERT-2022-1552 dfn-cert: DFN-CERT-2022-1516 dfn-cert: DFN-CERT-2022-1493 dfn-cert: DFN-CERT-2022-1473 dfn-cert: DFN-CERT-2022-1288

High (CVSS: 8.1) NVT: PHP < 8.0.28, 8.1.x < 8.1.16, 8.2.x < 8.2.3 Security Update - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 8.0.28 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 8.0.28, 8.1.16, 8.2.3 or later.
Affected Software/OS PHP versions prior to 8.0.28, 8.1.x prior to 8.1.16 and 8.2.x prior to 8.2.3.
Vulnerability Insight The following flaws exist:
... continues on next page ...

...continued from previous page...
<ul style="list-style-type: none"> - CVE-2023-0567: Fixed bug #81744 (Password_verify() always return true with some hash) - CVE-2023-0568: Fixed bug #81746 (1-byte array overrun in common path resolve code) - CVE-2023-0662: Fixed bug GHSA-54hq-v5wp-fqgv (DOS vulnerability when parsing multipart request body)
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: PHP < 8.0.28, 8.1.x < 8.1.16, 8.2.x < 8.2.3 Security Update - Linux</p> <p>OID:1.3.6.1.4.1.25623.1.0.104541</p> <p>Version used: 2023-10-13T05:06:10Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:php:php:7.2.34</p> <p>Method: PHP Detection (HTTP)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>References</p> <p>cve: CVE-2023-0567</p> <p>cve: CVE-2023-0568</p> <p>cve: CVE-2023-0662</p> <p>url: https://www.php.net/ChangeLog-8.php#8.2.3</p> <p>url: https://www.php.net/ChangeLog-8.php#8.1.16</p> <p>url: https://www.php.net/ChangeLog-8.php#8.0.28</p> <p>url: https://www.php.net/archive/2023.php#2023-02-14-2</p> <p>url: https://www.php.net/archive/2023.php#2023-02-14-3</p> <p>url: https://www.php.net/archive/2023.php#2023-02-14-1</p> <p>url: http://bugs.php.net/81744</p> <p>url: http://bugs.php.net/81746</p> <p>url: https://github.com/php/php-src/security/advisories/GHSA-54hq-v5wp-fqgv</p> <p>url: https://github.com/php/php-src/security/advisories/GHSA-7fj2-8x79-rj4</p> <p>cert-bund: WID-SEC-2023-2671</p> <p>cert-bund: WID-SEC-2023-1424</p> <p>cert-bund: WID-SEC-2023-1022</p> <p>cert-bund: WID-SEC-2023-0383</p> <p>dfn-cert: DFN-CERT-2024-3330</p> <p>dfn-cert: DFN-CERT-2024-2681</p> <p>dfn-cert: DFN-CERT-2023-2570</p> <p>dfn-cert: DFN-CERT-2023-2538</p> <p>dfn-cert: DFN-CERT-2023-0994</p> <p>dfn-cert: DFN-CERT-2023-0884</p> <p>dfn-cert: DFN-CERT-2023-0462</p> <p>dfn-cert: DFN-CERT-2023-0435</p> <p>dfn-cert: DFN-CERT-2023-0336</p>

High (CVSS: 7.8) NVT: PHP < 8.0.27, 8.1.x < 8.1.14, 8.2.x < 8.2.1 Security Update - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to an integer overflow vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 8.0.27 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 8.0.27, 8.1.14, 8.2.1 or later.
Affected Software/OS PHP prior to version 8.0.27, version 8.1.x through 8.1.13 and 8.2.0.
Vulnerability Insight Due to an uncaught integer overflow, PDO::quote() of PDO_SQLite may return a not properly quoted string.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 8.0.27, 8.1.x < 8.1.14, 8.2.x < 8.2.1 Security Update - Linux OID:1.3.6.1.4.1.25623.1.0.149069 Version used: 2023-01-09T10:12:48Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2022-31631 url: https://www.php.net/ChangeLog-8.php#8.0.27 url: https://www.php.net/ChangeLog-8.php#8.1.14 url: https://www.php.net/ChangeLog-8.php#8.2.1 ... continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2023-0035
dfn-cert: DFN-CERT-2023-0435
dfn-cert: DFN-CERT-2023-0422
dfn-cert: DFN-CERT-2023-0071
dfn-cert: DFN-CERT-2023-0034

High (CVSS: 7.5) NVT: Apache HTTP Server < 2.4.58 'mod_macro' Out-of-bounds Read Vulnerability - Linux
Product detection result cpe:/a:apache:http_server:2.4.52 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1 ↔.0.117232)
Summary Apache HTTP Server is prone to an out-of-bounds read vulnerability in mod_macro.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 2.4.52 Fixed version: 2.4.58 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 2.4.58 or later.
Affected Software/OS Apache HTTP Server version 2.4.57 and prior.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server < 2.4.58 'mod_macro' Out-of-bounds Read Vulnerability - Linux OID:1.3.6.1.4.1.25623.1.0.100272 Version used: 2024-02-15T05:05:40Z
Product Detection Result Product: cpe:/a:apache:http_server:2.4.52 Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)
... continues on next page ...

...continued from previous page ...

References

cve: CVE-2023-31122
url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.58
url: <https://www.openwall.com/lists/oss-security/2023/10/19/4>
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0899
cert-bund: WID-SEC-2024-0869
cert-bund: WID-SEC-2024-0769
cert-bund: WID-SEC-2024-0107
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2712
dfn-cert: DFN-CERT-2024-1411
dfn-cert: DFN-CERT-2024-1010
dfn-cert: DFN-CERT-2024-1000
dfn-cert: DFN-CERT-2024-0732
dfn-cert: DFN-CERT-2023-2640
dfn-cert: DFN-CERT-2023-2583

High (CVSS: 7.5)

NVT: Apache HTTP Server < 2.4.59 Multiple Vulnerabilities - Linux

Product detection result

cpe:/a:apache:http_server:2.4.52
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↔.0.117232)

Summary

Apache HTTP Server is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 2.4.52
Fixed version: 2.4.59
Installation
path / port: 80/tcp

Solution:

Solution type: VendorFix
Update to version 2.4.59 or later.

Affected Software/OS

Apache HTTP Server version 2.4.58 and prior.

Vulnerability Insight

... continues on next page ...

...continued from previous page ...
<p>The following vulnerabilities exist:</p> <ul style="list-style-type: none"> - CVE-2023-38709: HTTP response splitting - CVE-2024-24795: HTTP response splitting in multiple modules - CVE-2024-27316: HTTP/2 DoS by memory exhaustion on endless continuation frames
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Apache HTTP Server < 2.4.59 Multiple Vulnerabilities - Linux</p> <p>OID:1.3.6.1.4.1.25623.1.0.152039</p> <p>Version used: 2024-06-07T05:05:42Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:apache:http_server:2.4.52</p> <p>Method: Apache HTTP Server Detection Consolidation</p> <p>OID: 1.3.6.1.4.1.25623.1.0.117232)</p>
<p>References</p> <p>cve: CVE-2023-38709</p> <p>cve: CVE-2024-24795</p> <p>cve: CVE-2024-27316</p> <p>url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.59</p> <p>url: https://kb.cert.org/vuls/id/421644</p> <p>url: https://nowotarski.info/http2-continuation-flood/</p> <p>url: https://nowotarski.info/http2-continuation-flood-technical-details/</p> <p>cert-bund: WID-SEC-2024-1725</p> <p>cert-bund: WID-SEC-2024-1643</p> <p>cert-bund: WID-SEC-2024-1642</p> <p>cert-bund: WID-SEC-2024-1504</p> <p>cert-bund: WID-SEC-2024-1248</p> <p>cert-bund: WID-SEC-2024-1226</p> <p>cert-bund: WID-SEC-2024-0801</p> <p>cert-bund: WID-SEC-2024-0789</p> <p>dfn-cert: DFN-CERT-2024-2900</p> <p>dfn-cert: DFN-CERT-2024-2534</p> <p>dfn-cert: DFN-CERT-2024-2076</p> <p>dfn-cert: DFN-CERT-2024-1958</p> <p>dfn-cert: DFN-CERT-2024-1853</p> <p>dfn-cert: DFN-CERT-2024-1749</p> <p>dfn-cert: DFN-CERT-2024-1697</p> <p>dfn-cert: DFN-CERT-2024-1411</p> <p>dfn-cert: DFN-CERT-2024-1335</p> <p>dfn-cert: DFN-CERT-2024-1238</p> <p>dfn-cert: DFN-CERT-2024-1031</p> <p>dfn-cert: DFN-CERT-2024-1010</p> <p>dfn-cert: DFN-CERT-2024-0964</p> <p>dfn-cert: DFN-CERT-2024-0901</p>
...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2024-0890

High (CVSS: 7.5)

NVT: PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 NULL Deference Vulnerability (Feb 2021) - Linux

Product detection result

cpe:/a:php:php:7.2.34

Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

PHP is prone to a NULL dereference vulnerability in the SoapClient.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 7.2.34

Fixed version: 7.3.27

Installation

path / port: 80/tcp

Solution:**Solution type:** VendorFix

Update to version 7.3.27, 7.4.15, 8.0.2 or later.

Affected Software/OS

PHP versions prior to 7.3.27, 7.4.x prior to 7.4.15 and 8.0.x prior to 8.0.2.

Vulnerability Detection Method

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

Details: PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 NULL Deference Vulnerability (Feb 2021) - Linux

OID:1.3.6.1.4.1.25623.1.0.145323

Version used: 2021-11-29T15:00:35Z

Product Detection Result

Product: cpe:/a:php:php:7.2.34

Method: PHP Detection (HTTP)

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

cve: CVE-2021-21702

url: <https://www.php.net/ChangeLog-7.php#7.3.27>

... continues on next page ...

...continued from previous page ...
url: https://www.php.net/ChangeLog-7.php#7.4.15 url: https://www.php.net/ChangeLog-8.php#8.0.2 cert-bund: WID-SEC-2023-1737 cert-bund: WID-SEC-2022-2113 cert-bund: CB-K21/0124 dfn-cert: DFN-CERT-2023-1600 dfn-cert: DFN-CERT-2022-2639 dfn-cert: DFN-CERT-2022-2638 dfn-cert: DFN-CERT-2022-0904 dfn-cert: DFN-CERT-2021-2373 dfn-cert: DFN-CERT-2021-1645 dfn-cert: DFN-CERT-2021-1509 dfn-cert: DFN-CERT-2021-1453 dfn-cert: DFN-CERT-2021-0556 dfn-cert: DFN-CERT-2021-0380 dfn-cert: DFN-CERT-2021-0246

High (CVSS: 7.5)

NVT: PHP 'CVE-2017-7189' Improper Input Validation Vulnerability - Linux

Product detection result

cpe:/a:php:php:7.2.34

Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

PHP is improperly validating input from untrusted input.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 7.2.34

Fixed version: None

Installation

path / port: 80/tcp

Solution:

Solution type: WillNotFix

No solution was made available by the vendor. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Note: PHP versions 7.0.18 and 7.1.4 introduced a fix which was reverted again in version 7.0.19 / 7.1.5 respectively and the fix wasn't introduced again as of today (08-2020).

Affected Software/OS

All PHP versions since 4.3.0 up to the latest 7.x versions.

... continues on next page ...

...continued from previous page ...
Note: PHP versions 7.0.18 and 7.1.4 introduced a fix which was reverted again in version 7.0.19 / 7.1.5 respectively.
Vulnerability Insight main/streams/xp_socket.c in PHP misparses fsockopen calls, such as by interpreting fsockopen('127.0.0.1:80', 443) as if the address/port were 127.0.0.1:80:443, which is later truncated to 127.0.0.1:80. This behavior has a security risk if the explicitly provided port number (i.e., 443 in this example) is hardcoded into an application as a security policy, but the hostname argument (i.e., 127.0.0.1:80 in this example) is obtained from untrusted input.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP 'CVE-2017-7189' Improper Input Validation Vulnerability - Linux OID:1.3.6.1.4.1.25623.1.0.108874 Version used: 2024-02-15T05:05:40Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2017-7189 url: https://bugs.php.net/bug.php?id=74192 url: https://bugs.php.net/bug.php?id=74429 url: https://github.com/php/php-src/commit/bab0b99f376dac9170ac81382a5ed526938d5c95a
High (CVSS: 7.5) NVT: Apache HTTP Server 2.4.30 - 2.4.55 HTTP Request Smuggling Vulnerability - Linux
Product detection result cpe:/a:apache:http_server:2.4.52 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.117232)
Summary Apache HTTP Server is prone to a HTTP request smuggling vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 2.4.52 Fixed version: 2.4.56 Installation
... continues on next page ...

...continued from previous page ...	
path / port:	80/tcp
Solution: Solution type: VendorFix Update to version 2.4.56 or later.	
Affected Software/OS Apache HTTP Server versions 2.4.30 through 2.4.55.	
Vulnerability Insight HTTP Response Smuggling vulnerability via mod_proxy_uwsgi. Special characters in the origin response header can truncate/split the response forwarded to the client.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server 2.4.30 - 2.4.55 HTTP Request Smuggling Vulnerability - Linux OID:1.3.6.1.4.1.25623.1.0.104599 Version used: 2024-02-15T05:05:40Z	
Product Detection Result Product: cpe:/a:apache:http_server:2.4.52 Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)	
References cve: CVE-2023-27522 url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.56 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2023-2031 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-0583 dfn-cert: DFN-CERT-2024-1808 dfn-cert: DFN-CERT-2023-1895 dfn-cert: DFN-CERT-2023-0658 dfn-cert: DFN-CERT-2023-0546	
High (CVSS: 7.0) NVT: PHP 5.3.7 - 7.3.31, 7.4.x < 7.4.25, 8.0.x < 8.0.12 Security Update (Oct 2021) - Linux	
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)	
... continues on next page ...	

...continued from previous page ...
Summary PHP released new versions which includes a security fix.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.3.32 (not released yet) Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 7.3.32 (not released yet), 7.4.25, 8.0.12 or later.
Affected Software/OS PHP versions 5.3.7 through 7.3.31, 7.4.x through 7.4.24 and 8.0.x through 8.0.11. Note: While the referenced CVE is only listing PHP 7.3.x, 7.4.x and 8.0.x as affected the security research team is stating in the linked blog post that all versions down to 5.3.7 are affected.
Vulnerability Insight Fixed bug #81026 (PHP-FPM oob R/W in root process leading to privilege escalation).
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP 5.3.7 - 7.3.31, 7.4.x < 7.4.25, 8.0.x < 8.0.12 Security Update (Oct 2021) -. ↪.. OID:1.3.6.1.4.1.25623.1.0.117752 Version used: 2021-11-05T03:03:34Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2021-21703 url: https://www.php.net/ChangeLog-7.php#7.3.32 url: https://www.php.net/ChangeLog-7.php#7.4.25 url: https://www.php.net/ChangeLog-8.php#8.0.12 url: http://bugs.php.net/81026 url: https://www.ambionics.io/blog/php-fpm-local-root cert-bund: WID-SEC-2023-1737 cert-bund: WID-SEC-2022-0624
...continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2022-0586
cert-bund: CB-K21/1106
dfn-cert: DFN-CERT-2023-1600
dfn-cert: DFN-CERT-2022-2639
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2022-2337
dfn-cert: DFN-CERT-2022-1493
dfn-cert: DFN-CERT-2022-1046
dfn-cert: DFN-CERT-2022-0485
dfn-cert: DFN-CERT-2021-2586
dfn-cert: DFN-CERT-2021-2474
dfn-cert: DFN-CERT-2021-2200

[\[return to 10.0.0.92 \]](#)

2.2.2 High 3128/tcp

High (CVSS: 7.8) NVT: Squid DoS Vulnerability (GHSA-72c2-c3wm-8qxc, SQUID-2024:1)
Product detection result cpe:/a:squid-cache:squid:5.9 Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)
Summary Squid is prone to a denial of service (DoS) vulnerability in the HTTP Chunked Decoding.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 5.9 Fixed version: 6.8 Installation path / port: 3128/tcp
Solution: Solution type: VendorFix Update to version 6.8 or later.
Affected Software/OS Squid version 3.5.27 through 6.7.
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
<p>Due to an Uncontrolled Recursion bug, Squid may be vulnerable to a Denial of Service attack against HTTP Chunked decoder.</p> <p>This flaw was part of the 'Squid Caching Proxy Security Audit: 55 vulnerabilities and 35 0days' publication in October 2023 and filed as 'Chunked Encoding Stack Overflow'.</p>
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Squid DoS Vulnerability (GHSA-72c2-c3wm-8qxc, SQUID-2024:1)</p> <p>OID:1.3.6.1.4.1.25623.1.0.114405</p> <p>Version used: 2024-11-01T05:05:36Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:squid-cache:squid:5.9</p> <p>Method: Squid Detection (HTTP)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.900611)</p>
<p>References</p> <p>cve: CVE-2024-25111</p> <p>url: https://github.com/squid-cache/squid/security/advisories/GHSA-72c2-c3wm-8qxc ↩c</p> <p>url: https://megamansec.github.io/Squid-Security-Audit/</p> <p>url: https://joshua.hu/squid-security-audit-35-0days-45-exploits</p> <p>url: https://www.openwall.com/lists/oss-security/2023/10/11/3</p> <p>url: https://gist.github.com/rousskov/9af0d33d2a1f4b5b3b948b2da426e77d</p> <p>url: https://megamansec.github.io/Squid-Security-Audit/chunked-stackoverflow.htm ↩l</p> <p>cert-bund: WID-SEC-2024-0544</p> <p>dfn-cert: DFN-CERT-2024-2191</p> <p>dfn-cert: DFN-CERT-2024-1017</p> <p>dfn-cert: DFN-CERT-2024-0956</p> <p>dfn-cert: DFN-CERT-2024-0894</p> <p>dfn-cert: DFN-CERT-2024-0797</p> <p>dfn-cert: DFN-CERT-2024-0742</p> <p>dfn-cert: DFN-CERT-2024-0642</p>
<p>High (CVSS: 7.8)</p> <p>NVT: Squid DoS Vulnerability (GHSA-jm7h-w5q5-jpq9, SQUID-2020:13)</p>
<p>Product detection result</p> <p>cpe:/a:squid-cache:squid:5.9</p> <p>Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)</p>
<p>Summary</p> <p>Squid is prone to a denial of service (DoS) vulnerability.</p>
... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 5.9 Fixed version: 6.0.1 Installation path / port: 3128/tcp
Solution: Solution type: VendorFix Update to version 6.0.1 or later. As a workaround reject all gopher URL requests. Please see the referenced vendor advisory for more information.
Affected Software/OS Squid prior to version 6.0.1.
Vulnerability Insight This problem allows a remote gopher: server to trigger a buffer overflow by delivering large gopher protocol responses. On most operating systems with memory protection this will halt Squid service immediately, causing a denial of service to all Squid clients. The gopher protocol is always available and enabled in Squid prior to Squid 6.0.1.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Squid DoS Vulnerability (GHSA-jm7h-w5q5-jpq9, SQUID-2020:13) OID:1.3.6.1.4.1.25623.1.0.150942 Version used: 2023-09-08T05:06:21Z
Product Detection Result Product: cpe:/a:squid-cache:squid:5.9 Method: Squid Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.900611)
References url: https://github.com/squid-cache/squid/security/advisories/GHSA-jm7h-w5q5-jpq9 ↪9

High (CVSS: 7.8)
 NVT: Squid Multiple 0-Day Vulnerabilities (Oct 2023)

Product detection result
 cpe:/a:squid-cache:squid:5.9
 Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)

... continues on next page ...

...continued from previous page ...
Summary Squid is prone to multiple zero-day (0-day) vulnerabilities.
Quality of Detection (QoD): 70%
Vulnerability Detection Result Installed version: 5.9 Fixed version: None Installation path / port: 3128/tcp
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. Notes: - It seems that some of the flaws could be mitigated by workarounds (listed in the referenced GitHub Gist) via either configuration changes and/or by disabling some features / functionality of Squid during build time - If only these workarounds have been applied and the risk is accepted that these workarounds might not fully mitigate the relevant flaw(s) please create an override for this result
Affected Software/OS As of 10/2024 the situation about the versions affected by the previous listed vulnerabilities is largely unclear (The security researcher only stated that all vulnerabilities were discovered in squid-5.0.5 and the vendor only published a few advisories so far). Due to this unclear situation all Squid versions are currently assumed to be vulnerable by the not yet fixed flaws.
Vulnerability Insight The following flaws have been reported in 2021 to the vendor and seems to be not fixed yet: - One-Byte Buffer OverRead in HTTP Request Header Parsing - strlen(NULL) Crash Using Digest Authentication GHSA-254c-93q9-cp53 - Gopher Assertion Crash - Whois Assertion Crash - RFC 2141 / 2169 (URN) Assertion Crash - Assertion in Negotiate/NTLM Authentication Using Pipeline Prefetching - Assertion on IPv6 Host Requests with --disable-ipv6 - Assertion Crash on Unexpected 'HTTP/1.1 100 Continue' Response Header - Pipeline Prefetch Assertion With Double 'Expect:100-continue' Request Headers - Pipeline Prefetch Assertion With Invalid Headers - Assertion Crash in Deferred Requests - Assertion in Digest Authentication
... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - FTP Authentication Crash - Assertion Crash In HTTP Response Headers Handling - Implicit Assertion in Stream Handling <p>Note: One GHSA advisory has been provided by the security researcher but is not published / available yet.</p>
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Squid Multiple 0-Day Vulnerabilities (0ct 2023)</p> <p>OID:1.3.6.1.4.1.25623.1.0.100439</p> <p>Version used: 2024-11-01T05:05:36Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:squid-cache:squid:5.9</p> <p>Method: Squid Detection (HTTP)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.900611)</p>
<p>References</p> <p>url: https://megamansec.github.io/Squid-Security-Audit/</p> <p>url: https://joshua.hu/squid-security-audit-35-0days-45-exploits</p> <p>url: https://www.openwall.com/lists/oss-security/2023/10/11/3</p> <p>url: https://gist.github.com/rousskov/9af0d33d2a1f4b5b3b948b2da426e77d</p>

<p>High (CVSS: 7.5)</p> <p>NVT: Squid Multiple DoS Vulnerabilities (GHSA-543m-w2m2-g255, SQUID-2023:2)</p>
<p>Product detection result</p> <p>cpe:/a:squid-cache:squid:5.9</p> <p>Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)</p>
<p>Summary</p> <p>Squid is prone to multiple denial of service (DoS) vulnerabilities.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 5.9</p> <p>Fixed version: 6.4</p> <p>Installation</p> <p>path / port: 3128/tcp</p>
<p>Solution:</p> <p>Solution type: VendorFix</p> <p>Update to version 6.4 or later.</p>
... continues on next page ...

...continued from previous page ...
Affected Software/OS Squid versions prior to 6.4.
Vulnerability Insight The following flaws exist: <ul style="list-style-type: none">- Due to an Improper Handling of Structural Elements bug Squid is vulnerable to a Denial of Service attack against HTTP and HTTPS clients.- Due to an Incomplete Filtering of Special Elements bug Squid is vulnerable to a Denial of Service attack against HTTP and HTTPS clients. These flaws were part of the 'Squid Caching Proxy Security Audit: 55 vulnerabilities and 35 0days' publication in October 2023 and filed as 'Cache Poisoning by Large Stored Response Headers (With Bonus XSS)'.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Squid Multiple DoS Vulnerabilities (GHSA-543m-w2m2-g255, SQUID-2023:2) OID:1.3.6.1.4.1.25623.1.0.100705 Version used: 2024-11-01T05:05:36Z
Product Detection Result Product: cpe:/a:squid-cache:squid:5.9 Method: Squid Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.900611)
References cve: CVE-2023-5824 url: https://github.com/squid-cache/squid/security/advisories/GHSA-543m-w2m2-g255 ↩5 url: https://megamansec.github.io/Squid-Security-Audit/ url: https://joshua.hu/squid-security-audit-35-0days-45-exploits url: https://www.openwall.com/lists/oss-security/2023/10/11/3 url: https://gist.github.com/rousskov/9af0d33d2a1f4b5b3b948b2da426e77d url: https://megamansec.github.io/Squid-Security-Audit/cache-headers.html cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2023-2725 dfn-cert: DFN-CERT-2024-0956 dfn-cert: DFN-CERT-2024-0214 dfn-cert: DFN-CERT-2024-0038 dfn-cert: DFN-CERT-2023-2949
High (CVSS: 7.5) NVT: Squid DoS Vulnerability (GHSA-8w9r-p88v-mmx9, SQUID-2023:7)
Product detection result
... continues on next page ...

...continued from previous page ...
cpe:/a:squid-cache:squid:5.9 Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)
Summary Squid is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 5.9 Fixed version: 6.5 Installation path / port: 3128/tcp
Solution: Solution type: VendorFix Update to version 6.5 or later.
Affected Software/OS Squid versions 2.2 through 5.9 and 6.0 through 6.4.
Vulnerability Insight Due to a Buffer Overread bug Squid is vulnerable to a Denial of Service attack against Squid HTTP Message processing. This flaw was part of the 'Squid Caching Proxy Security Audit: 55 vulnerabilities and 35 0days' publication in October 2023 and filed as '1-Byte Buffer OverRead in RFC 1123 date/time Handling'.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Squid DoS Vulnerability (GHSA-8w9r-p88v-mmx9, SQUID-2023:7) OID:1.3.6.1.4.1.25623.1.0.114206 Version used: 2024-11-01T05:05:36Z
Product Detection Result Product: cpe:/a:squid-cache:squid:5.9 Method: Squid Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.900611)
References cve: CVE-2023-49285 url: https://github.com/squid-cache/squid/security/advisories/GHSA-8w9r-p88v-mmx9 url: https://megamansec.github.io/Squid-Security-Audit/
... continues on next page ...

...continued from previous page ...
url: https://joshua.hu/squid-security-audit-35-0days-45-exploits
url: https://www.openwall.com/lists/oss-security/2023/10/11/3
url: https://gist.github.com/rousskov/9af0d33d2a1f4b5b3b948b2da426e77d
url: https://megamansec.github.io/Squid-Security-Audit/datetime-overflow.html
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2023-3049
dfn-cert: DFN-CERT-2024-1684
dfn-cert: DFN-CERT-2024-0970
dfn-cert: DFN-CERT-2024-0642
dfn-cert: DFN-CERT-2024-0214
dfn-cert: DFN-CERT-2024-0172
dfn-cert: DFN-CERT-2024-0039
dfn-cert: DFN-CERT-2024-0038
dfn-cert: DFN-CERT-2024-0026
dfn-cert: DFN-CERT-2023-3192
dfn-cert: DFN-CERT-2023-3036

High (CVSS: 7.5)

NVT: Squid DoS Vulnerability (GHSA-cg5h-v6vc-w33f, SQUID-2021:8)

Product detection result

cpe:/a:squid-cache:squid:5.9

Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)

Summary

Squid is prone to a denial of service (DoS) vulnerability in the Gopher gateway.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 5.9

Fixed version: 6.0.1

Installation

path / port: 3128/tcp

Solution:

Solution type: VendorFix

Update to version 6.0.1 or later.

As a workaround reject all gopher URL requests. Please see the referenced vendor advisory for more information.

Note: Removing the gopher port 70 from the Safe_ports ACL is not sufficient to avoid this vulnerability.

Affected Software/OS

... continues on next page ...

...continued from previous page ...
Squid version 2.x and later prior to version 6.0.1.
<p>Vulnerability Insight</p> <p>Due to a NULL pointer dereference bug Squid is vulnerable to a Denial of Service attack against Squid's Gopher gateway.</p> <p>The gopher protocol is always available and enabled in Squid prior to Squid 6.0.1.</p> <p>Responses triggering this bug are possible to be received from any gopher server, even those without malicious intent.</p> <p>This flaw was part of the 'Squid Caching Proxy Security Audit: 55 vulnerabilities and 35 0days' publication in October 2023 and filed as 'Null Pointer Dereference in Gopher Response Handling'.</p>
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Squid DoS Vulnerability (GHSA-cg5h-v6vc-w33f, SQUID-2021:8)</p> <p>OID:1.3.6.1.4.1.25623.1.0.151071</p> <p>Version used: 2024-11-01T05:05:36Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:squid-cache:squid:5.9</p> <p>Method: Squid Detection (HTTP)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.900611)</p>
<p>References</p> <p>cve: CVE-2023-46728</p> <p>url: https://github.com/squid-cache/squid/security/advisories/GHSA-cg5h-v6vc-w33f</p> <p>url: https://megamansec.github.io/Squid-Security-Audit/</p> <p>url: https://joshua.hu/squid-security-audit-35-0days-45-exploits</p> <p>url: https://www.openwall.com/lists/oss-security/2023/10/11/3</p> <p>url: https://gist.github.com/rousskov/9af0d33d2a1f4b5b3b948b2da426e77d</p> <p>url: https://megamansec.github.io/Squid-Security-Audit/gopher-nullpointer.html</p> <p>cert-bund: WID-SEC-2024-1248</p> <p>cert-bund: WID-SEC-2023-2837</p> <p>dfn-cert: DFN-CERT-2024-0970</p> <p>dfn-cert: DFN-CERT-2024-0214</p> <p>dfn-cert: DFN-CERT-2024-0039</p> <p>dfn-cert: DFN-CERT-2024-0038</p> <p>dfn-cert: DFN-CERT-2024-0026</p> <p>dfn-cert: DFN-CERT-2023-3192</p> <p>dfn-cert: DFN-CERT-2023-2956</p> <p>dfn-cert: DFN-CERT-2023-2934</p>
High (CVSS: 7.5)
NVT: Squid DoS Vulnerability (GHSA-h5x6-w8mv-xfpr, SQUID-2024:2)
Product detection result
... continues on next page ...

...continued from previous page ...
cpe:/a:squid-cache:squid:5.9 Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)
Summary Squid is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 5.9 Fixed version: 6.5 Installation path / port: 3128/tcp
Solution: Solution type: VendorFix Update to version 6.5 or later.
Affected Software/OS Squid versions prior to 6.5.
Vulnerability Insight Due to a Collapse of Data into Unsafe Value bug, Squid may be vulnerable to a Denial of Service attack against HTTP header parsing. This flaw was part of the 'Squid Caching Proxy Security Audit: 55 vulnerabilities and 35 0days' publication in October 2023 and filed as 'Memory Leak in HTTP Response Parsing'.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Squid DoS Vulnerability (GHSA-h5x6-w8mv-xfpr, SQUID-2024:2) OID:1.3.6.1.4.1.25623.1.0.151739 Version used: 2025-01-13T08:32:03Z
Product Detection Result Product: cpe:/a:squid-cache:squid:5.9 Method: Squid Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.900611)
References cve: CVE-2024-25617 url: https://github.com/squid-cache/squid/security/advisories/GHSA-h5x6-w8mv-xfpr ↔ url: https://megamansec.github.io/Squid-Security-Audit/ url: https://joshua.hu/squid-security-audit-35-0days-45-exploits
... continues on next page ...

...continued from previous page ...
url: https://www.openwall.com/lists/oss-security/2023/10/11/3
url: https://gist.github.com/rousskov/9af0d33d2a1f4b5b3b948b2da426e77d
url: https://megamansec.github.io/Squid-Security-Audit/response-memleaks.html
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-0396
dfn-cert: DFN-CERT-2024-1684
dfn-cert: DFN-CERT-2024-0970
dfn-cert: DFN-CERT-2024-0956
dfn-cert: DFN-CERT-2024-0894
dfn-cert: DFN-CERT-2024-0742
dfn-cert: DFN-CERT-2024-0642
dfn-cert: DFN-CERT-2024-0554
dfn-cert: DFN-CERT-2024-0491

High (CVSS: 7.5)

NVT: Squid DoS Vulnerability (GHSA-73m6-jm96-c6r3, SQUID-2023:4)

Product detection result

cpe:/a:squid-cache:squid:5.9

Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)

Summary

Squid is prone to a denial of service (DoS) vulnerability in the SSL Certificate validation.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 5.9

Fixed version: 6.4

Installation

path / port: 3128/tcp

Solution:

Solution type: VendorFix

Update to version 6.4 or later.

Affected Software/OS

Squid version 3.3.0.1 through 6.3.

Vulnerability Insight

Due to an Improper Validation of Specified Index bug Squid is vulnerable to a Denial of Service attack against SSL Certificate validation.

This flaw was part of the 'Squid Caching Proxy Security Audit: 55 vulnerabilities and 35 0days' publication in October 2023 and filed as 'Buffer UnderRead in SSL CN Parsing'.

... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Squid DoS Vulnerability (GHSA-73m6-jm96-c6r3, SQUID-2023:4) OID:1.3.6.1.4.1.25623.1.0.151251 Version used: 2024-11-01T05:05:36Z
Product Detection Result Product: cpe:/a:squid-cache:squid:5.9 Method: Squid Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.900611)
References cve: CVE-2023-46724 url: https://github.com/squid-cache/squid/security/advisories/GHSA-73m6-jm96-c6r3 ↪3 url: https://megamansec.github.io/Squid-Security-Audit/ url: https://joshua.hu/squid-security-audit-35-0days-45-exploits url: https://www.openwall.com/lists/oss-security/2023/10/11/3 url: https://gist.github.com/rousskov/9af0d33d2a1f4b5b3b948b2da426e77d url: https://megamansec.github.io/Squid-Security-Audit/ssl-bufferunderread.html cert-bund: WID-SEC-2023-2801 dfn-cert: DFN-CERT-2024-0970 dfn-cert: DFN-CERT-2024-0642 dfn-cert: DFN-CERT-2024-0214 dfn-cert: DFN-CERT-2024-0038 dfn-cert: DFN-CERT-2024-0026 dfn-cert: DFN-CERT-2023-3192 dfn-cert: DFN-CERT-2023-2934 dfn-cert: DFN-CERT-2023-2746
High (CVSS: 7.5) NVT: Squid Multiple DoS Vulnerabilities (GHSA-f975-v7qw-q7hj, SQUID-2024:4)
Product detection result cpe:/a:squid-cache:squid:5.9 Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)
Summary Squid is prone to multiple denial of service (DoS) vulnerabilities due to multiple issues in ESI.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 5.9
... continues on next page ...

...continued from previous page ...	
Fixed version:	7.0
Installation path / port:	3128/tcp
Solution: Solution type: VendorFix Update to version 7.0 or later.	
Affected Software/OS Squid version 3.0 through 6.x.	
Vulnerability Insight Due to Input Validation, Premature Release of Resource During Expected Lifetime, and Missing Release of Resource after Effective Lifetime bugs, Squid is vulnerable to Denial of Service attacks by a trusted server against all clients using the proxy. These flaws were part of the 'Squid Caching Proxy Security Audit: 55 vulnerabilities and 35 0days' publication in October 2023 and filed as: - Memory Leak in ESI Error Processing - Assertion in ESI Header Handling - Use-After-Free in ESI 'Try' (and 'Choose') Processing - Use-After-Free in ESI Expression Evaluation - Assertion Due to 0 ESI 'when' Checking - Assertion Using ESI's When Directive - Assertion in ESI Variable Assignment (String) - Assertion in ESI Variable Assignment - Null Pointer Dereference In ESI's esi:include and esi:when	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Squid Multiple DoS Vulnerabilities (GHSA-f975-v7qw-q7hj, SQUID-2024:4) OID:1.3.6.1.4.1.25623.1.0.114851 Version used: 2024-11-07T05:05:35Z	
Product Detection Result Product: cpe:/a:squid-cache:squid:5.9 Method: Squid Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.900611)	
References cve: CVE-2024-45802 url: https://github.com/squid-cache/squid/security/advisories/GHSA-f975-v7qw-q7hj ↩j url: https://megamansec.github.io/Squid-Security-Audit/ url: https://joshua.hu/squid-security-audit-35-0days-45-exploits url: https://www.openwall.com/lists/oss-security/2023/10/11/3	
...continues on next page ...	

...continued from previous page ...
url: https://gist.github.com/rousskov/9af0d33d2a1f4b5b3b948b2da426e77d
url: https://megamansec.github.io/Squid-Security-Audit/esi-when-assert-0.html
url: https://megamansec.github.io/Squid-Security-Audit/esi-when-assert-1.html
url: https://megamansec.github.io/Squid-Security-Audit/esi-nullpointer.html
url: https://megamansec.github.io/Squid-Security-Audit/esi-uaf.html
url: https://megamansec.github.io/Squid-Security-Audit/esi-assignassert.html
url: https://megamansec.github.io/Squid-Security-Audit/esi-assignassert-2.html
url: https://megamansec.github.io/Squid-Security-Audit/esi-uaf-crash.html
url: https://megamansec.github.io/Squid-Security-Audit/esi-memleak.html
url: https://megamansec.github.io/Squid-Security-Audit/esi-assert-header.html
cert-bund: WID-SEC-2024-3280
dfn-cert: DFN-CERT-2024-3050
dfn-cert: DFN-CERT-2024-2909

High (CVSS: 7.5) NVT: Squid Multiple DoS Vulnerabilities (GHSA-2g3c-pg7q-g59w, SQUID-2023:5)
Product detection result cpe:/a:squid-cache:squid:5.9 Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)
Summary Squid is prone to multiple denial of service (DoS) vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 5.9 Fixed version: 6.4 Installation path / port: 3128/tcp
Solution: Solution type: VendorFix Update to version 6.4 or later.
Affected Software/OS Squid versions 5.0.3 through 5.9 and 6.0 through 6.3.
Vulnerability Insight The following flaws exist: - Due to an Incorrect Conversion between Numeric Types bug Squid is vulnerable to a Denial of Service attack against FTP Native Relay input validation. - Due to an Incorrect Conversion between Numeric Types bug Squid is vulnerable to a Denial of Service attack against ftp:// URL validation and access control.
... continues on next page ...

...continued from previous page ...
These flaws were part of the 'Squid Caching Proxy Security Audit: 55 vulnerabilities and 35 0days' publication in October 2023 and filed as 'FTP URI Assertion'.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Squid Multiple DoS Vulnerabilities (GHSA-2g3c-pg7q-g59w, SQUID-2023:5) OID:1.3.6.1.4.1.25623.1.0.100664 Version used: 2024-11-01T05:05:36Z
Product Detection Result Product: cpe:/a:squid-cache:squid:5.9 Method: Squid Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.900611)
References cve: CVE-2023-46848 url: https://github.com/squid-cache/squid/security/advisories/GHSA-2g3c-pg7q-g59w url: https://megamansec.github.io/Squid-Security-Audit/ url: https://joshua.hu/squid-security-audit-35-0days-45-exploits url: https://www.openwall.com/lists/oss-security/2023/10/11/3 url: https://gist.github.com/rousskov/9af0d33d2a1f4b5b3b948b2da426e77d url: https://megamansec.github.io/Squid-Security-Audit/ftp-assert.html cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2023-2725 dfn-cert: DFN-CERT-2024-0642 dfn-cert: DFN-CERT-2023-2934 dfn-cert: DFN-CERT-2023-2746 dfn-cert: DFN-CERT-2023-2712
High (CVSS: 7.5) NVT: Squid DoS Vulnerability (GHSA-xggx-9329-3c27, SQUID-2023:8)
Product detection result cpe:/a:squid-cache:squid:5.9 Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)
Summary Squid is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 5.9 Fixed version: 6.5
... continues on next page ...

...continued from previous page ...	
Installation	
path / port:	3128/tcp
Solution:	
Solution type: VendorFix	
Update to version 6.5 or later.	
Affected Software/OS	
Squid versions prior to 6.5.	
Vulnerability Insight	
Due to an Incorrect Check of Function Return Value bug Squid is vulnerable to a Denial of Service attack against its Helper process management.	
This flaw was part of the 'Squid Caching Proxy Security Audit: 55 vulnerabilities and 35 0days' publication in October 2023 and filed as 'Assertion in Squid Helper Process Creator'.	
Vulnerability Detection Method	
Checks if a vulnerable version is present on the target host.	
Details: Squid DoS Vulnerability (GHSA-xggx-9329-3c27, SQUID-2023:8)	
OID:1.3.6.1.4.1.25623.1.0.114208	
Version used: 2024-11-01T05:05:36Z	
Product Detection Result	
Product: cpe:/a:squid-cache:squid:5.9	
Method: Squid Detection (HTTP)	
OID: 1.3.6.1.4.1.25623.1.0.900611)	
References	
url: https://megamansec.github.io/Squid-Security-Audit/ipc-assert.html	
cve: CVE-2023-49286	
url: https://github.com/squid-cache/squid/security/advisories/GHSA-xggx-9329-3c27	
url: https://megamansec.github.io/Squid-Security-Audit/	
url: https://joshua.hu/squid-security-audit-35-0days-45-exploits	
url: https://www.openwall.com/lists/oss-security/2023/10/11/3	
url: https://gist.github.com/rousskov/9af0d33d2a1f4b5b3b948b2da426e77d	
cert-bund: WID-SEC-2024-1248	
cert-bund: WID-SEC-2023-3049	
dfn-cert: DFN-CERT-2024-1684	
dfn-cert: DFN-CERT-2024-0970	
dfn-cert: DFN-CERT-2024-0642	
dfn-cert: DFN-CERT-2024-0214	
dfn-cert: DFN-CERT-2024-0172	
dfn-cert: DFN-CERT-2024-0039	
dfn-cert: DFN-CERT-2024-0038	
... continues on next page ...	

...continued from previous page ...	
dfn-cert: DFN-CERT-2024-0026	
dfn-cert: DFN-CERT-2023-3192	
dfn-cert: DFN-CERT-2023-3036	
High (CVSS: 7.5) NVT: Squid DoS Vulnerability (GHSA-wgq4-4cfg-c4x3, SQUID-2023:10)	
Product detection result cpe:/a:squid-cache:squid:5.9 Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)	
Summary Squid is prone to a denial of service (DoS) vulnerability.	
Quality of Detection (QoD): 30%	
Vulnerability Detection Result Installed version: 5.9 Fixed version: 6.6 Installation path / port: 3128/tcp	
Solution: Solution type: VendorFix Update to version 6.6 or later.	
Affected Software/OS Squid version 2.6 through 6.5.	
Vulnerability Insight Due to an uncontrolled recursion bug, Squid may be vulnerable to denial of service attack against HTTP request parsing. This flaw was part of the 'Squid Caching Proxy Security Audit: 55 vulnerabilities and 35 0days' publication in October 2023 and filed as 'X-Forwarded-For Stack Overflow'.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Squid DoS Vulnerability (GHSA-wgq4-4cfg-c4x3, SQUID-2023:10) OID:1.3.6.1.4.1.25623.1.0.151403 Version used: 2024-11-01T05:05:36Z	
Product Detection Result Product: cpe:/a:squid-cache:squid:5.9 Method: Squid Detection (HTTP)	
... continues on next page ...	

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.900611)
References cve: CVE-2023-50269 url: https://github.com/squid-cache/squid/security/advisories/GHSA-wgq4-4cfg-c4x ↪3 url: https://megamansec.github.io/Squid-Security-Audit/ url: https://joshua.hu/squid-security-audit-35-0days-45-exploits url: https://www.openwall.com/lists/oss-security/2023/10/11/3 url: https://gist.github.com/rousskov/9af0d33d2a1f4b5b3b948b2da426e77d url: https://megamansec.github.io/Squid-Security-Audit/xff-stackoverflow.html cert-bund: WID-SEC-2023-3150 dfn-cert: DFN-CERT-2024-1684 dfn-cert: DFN-CERT-2024-1413 dfn-cert: DFN-CERT-2024-0970 dfn-cert: DFN-CERT-2024-0742 dfn-cert: DFN-CERT-2024-0642 dfn-cert: DFN-CERT-2024-0290 dfn-cert: DFN-CERT-2024-0214 dfn-cert: DFN-CERT-2024-0172 dfn-cert: DFN-CERT-2024-0039 dfn-cert: DFN-CERT-2023-3192 dfn-cert: DFN-CERT-2023-3162

High (CVSS: 7.5)

NVT: Squid DoS Vulnerability (GHSA-rj5h-46j6-q2g5, SQUID-2023:9)

Product detection result

cpe:/a:squid-cache:squid:5.9

Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)

Summary

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

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 5.9

Fixed version: 6.0.1

Installation

path / port: 3128/tcp

Solution:**Solution type:** VendorFix

Update to version 6.0.1 or later.

... continues on next page ...

...continued from previous page ...
Affected Software/OS Squid versions 3.5 through 5.9.
Vulnerability Insight Due to a Use-After-Free bug Squid is vulnerable to a Denial of Service attack against collapsed forwarding. This flaw was part of the 'Squid Caching Proxy Security Audit: 55 vulnerabilities and 35 0days' publication in October 2023 and filed as 'Use-After-Free in TRACE Requests'.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Squid DoS Vulnerability (GHSA-rj5h-46j6-q2g5, SQUID-2023:9) OID:1.3.6.1.4.1.25623.1.0.114207 Version used: 2024-11-01T05:05:36Z
Product Detection Result Product: cpe:/a:squid-cache:squid:5.9 Method: Squid Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.900611)
References cve: CVE-2023-49288 url: https://github.com/squid-cache/squid/security/advisories/GHSA-rj5h-46j6-q2g5 url: https://megamansec.github.io/Squid-Security-Audit/ url: https://joshua.hu/squid-security-audit-35-0days-45-exploits url: https://www.openwall.com/lists/oss-security/2023/10/11/3 url: https://gist.github.com/rousskov/9af0d33d2a1f4b5b3b948b2da426e77d url: https://megamansec.github.io/Squid-Security-Audit/trace-uaf.html cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2023-3049 dfn-cert: DFN-CERT-2024-0956 dfn-cert: DFN-CERT-2023-3192
<div>High (CVSS: 7.5) NVT: Squid DoS Vulnerability (GHSA-phqj-m8gv-cq4g, SQUID-2023:3)</div>
Product detection result cpe:/a:squid-cache:squid:5.9 Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)
Summary
... continues on next page ...

...continued from previous page ...
Squid is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 5.9 Fixed version: 6.4 Installation path / port: 3128/tcp
Solution: Solution type: VendorFix Update to version 6.4 or later.
Affected Software/OS Squid versions 3.2.0.1 through 5.9 and 6.0 through 6.3.
Vulnerability Insight Due to a buffer overflow bug Squid is vulnerable to a Denial of Service attack against HTTP Digest Authentication. This flaw was part of the 'Squid Caching Proxy Security Audit: 55 vulnerabilities and 35 0days' publication in October 2023 and filed as 'Buffer Overflow in Digest Authentication'.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Squid DoS Vulnerability (GHSA-phqj-m8gv-cq4g, SQUID-2023:3) OID:1.3.6.1.4.1.25623.1.0.100832 Version used: 2024-11-01T05:05:36Z
Product Detection Result Product: cpe:/a:squid-cache:squid:5.9 Method: Squid Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.900611)
References cve: CVE-2023-46847 url: https://github.com/squid-cache/squid/security/advisories/GHSA-phqj-m8gv-cq4g url: https://megamansec.github.io/Squid-Security-Audit/ url: https://joshua.hu/squid-security-audit-35-0days-45-exploits url: https://www.openwall.com/lists/oss-security/2023/10/11/3 url: https://gist.github.com/rousskov/9af0d33d2a1f4b5b3b948b2da426e77d url: https://megamansec.github.io/Squid-Security-Audit/digest-overflow.html cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2023-2725
... continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2024-0642
dfn-cert: DFN-CERT-2024-0039
dfn-cert: DFN-CERT-2023-2934
dfn-cert: DFN-CERT-2023-2782
dfn-cert: DFN-CERT-2023-2781
dfn-cert: DFN-CERT-2023-2746
dfn-cert: DFN-CERT-2023-2712

[\[return to 10.0.0.92 \]](#)

2.2.3 High general/tcp

High (CVSS: 10.0) NVT: LibreOffice Unchecked Script Execution Vulnerability (Jul 2024) - Linux
Product detection result cpe:/a:libreoffice:libreoffice:7.3.7.2.2 Detected by LibreOffice Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.25623 ↪.1.0.902701)
Summary LibreOffice is prone to an unchecked script execution vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.3.7.2.2 Fixed version: 7.6.7 Installation path / port: /usr/bin/libreoffice
Impact Successful exploitation allows an attacker to create a document which without prompt will execute scripts built-into LibreOffice on clicking a graphic.
Solution: Solution type: VendorFix Update to version 7.6.7 or 24.2.3 later.
Affected Software/OS LibreOffice prior to version 7.6.7, 24.2.x prior to 24.2.3 on Linux.
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
The flaw exists due to an unchecked script execution error in LibreOffice Graphics on-click binding.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: LibreOffice Unchecked Script Execution Vulnerability (Jul 2024) - Linux OID:1.3.6.1.4.1.25623.1.0.834249 Version used: 2024-07-25T05:05:41Z
Product Detection Result Product: cpe:/a:libreoffice:libreoffice:7.3.7.2.2 Method: LibreOffice Detection (Linux/Unix SSH Login) OID: 1.3.6.1.4.1.25623.1.0.902701)
References cve: CVE-2024-3044 url: https://www.libreoffice.org/about-us/security/advisories/CVE-2024-3044 cert-bund: WID-SEC-2024-1144 dfn-cert: DFN-CERT-2024-1324

High (CVSS: 10.0) NVT: LibreOffice Improper Certificate Validation Vulnerability (Jul 2024) - Linux
Product detection result cpe:/a:libreoffice:libreoffice:7.3.7.2.2 Detected by LibreOffice Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.25623 ↪.1.0.902701)
Summary LibreOffice is prone to an improper certificate validation vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.3.7.2.2 Fixed version: 24.2.4 Installation path / port: /usr/bin/libreoffice
Impact Successful exploitation allows an attacker to perform man-in-the-middle attacks, potentially intercepting or modifying data transmitted between LibreOffice (when used in LibreOfficeKit mode) and remote servers.
... continues on next page ...

...continued from previous page ...
Solution: Solution type: VendorFix Update to version 24.2.4 or later.
Affected Software/OS LibreOffice prior to version 24.2.4 on Linux.
Vulnerability Insight The flaw exists due to TLS certificate is not properly verified when utilizing LibreOfficeKit.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: LibreOffice Improper Certificate Validation Vulnerability (Jul 2024) - Linux OID:1.3.6.1.4.1.25623.1.0.834217 Version used: 2024-07-25T05:05:41Z
Product Detection Result Product: cpe:/a:libreoffice:libreoffice:7.3.7.2.2 Method: LibreOffice Detection (Linux/Unix SSH Login) OID: 1.3.6.1.4.1.25623.1.0.902701)
References cve: CVE-2024-5261 url: https://www.libreoffice.org/about-us/security/advisories/cve-2024-5261 url: https://feedly.com/cve/CVE-2024-5261 cert-bund: WID-SEC-2024-1446 dfn-cert: DFN-CERT-2024-1731

High (CVSS: 10.0) NVT: PHP End of Life (EOL) Detection - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary The PHP version on the remote host has reached the end of life (EOL) and should not be used anymore.
Quality of Detection (QoD): 30%
Vulnerability Detection Result The "PHP" version on the remote host has reached the end of life.
... continues on next page ...

...continued from previous page ...	
CPE:	cpe:/a:php:php:7.2.34
Installed version:	7.2.34
EOL version:	7.2
EOL date:	2020-11-30
Impact An EOL version of PHP is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.	
Solution: Solution type: VendorFix Update the PHP version on the remote host to a still supported version.	
Vulnerability Insight Each release branch of PHP is fully supported for two years from its initial stable release. During this period, bugs and security issues that have been reported are fixed and are released in regular point releases. After this two year period of active support, each branch is then supported for an additional year for critical security issues only. Releases during this period are made on an as-needed basis: there may be multiple point releases, or none, depending on the number of reports. Once the three years of support are completed, the branch reaches its end of life and is no longer supported.	
Vulnerability Detection Method Checks if an EOL version is present on the target host. Details: PHP End of Life (EOL) Detection - Linux OID:1.3.6.1.4.1.25623.1.0.105889 Version used: 2024-02-28T14:37:42Z	
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)	
References url: https://secure.php.net/supported-versions.php url: https://secure.php.net/eol.php	
High (CVSS: 9.8) NVT: OpenBSD OpenSSH 8.9 - 9.2 Unspecified Vulnerability	
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)	
... continues on next page ...	

...continued from previous page ...
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.3 Installation path / port: /snap/core22/1612/usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.3 or later.
Affected Software/OS OpenBSD OpenSSH versions starting from 8.9 and prior to 9.3.
Vulnerability Insight ssh-add(1): when adding smartcard keys to ssh-agent(1) with the per-hop destination constraints (ssh-add -h ...) added in OpenSSH 8.9, a logic error prevented the constraints from being communicated to the agent. This resulted in the keys being added without constraints. The common cases of non-smartcard keys and keys without destination constraints are unaffected. This problem was reported by Luci Stanescu.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH 8.9 - 9.2 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104634 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2023-28531 url: https://www.openssh.com/releases/notes.html#9.3 url: https://www.openwall.com/lists/oss-security/2023/03/15/8 cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2023-0670 dfn-cert: DFN-CERT-2024-1260
... continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2024-0341 dfn-cert: DFN-CERT-2023-3218 dfn-cert: DFN-CERT-2023-3182 dfn-cert: DFN-CERT-2023-1424
High (CVSS: 9.8) NVT: Apache HTTP Server 2.4.0 - 2.4.55 HTTP Request Smuggling Vulnerability - Linux
Product detection result cpe:/a:apache:http_server:2.4.52 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1 ↔.0.117232)
Summary Apache HTTP Server is prone to a HTTP request smuggling vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 2.4.52 Fixed version: 2.4.56 Installation path / port: /usr/sbin/apache2
Impact Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning.
Solution: Solution type: VendorFix Update to version 2.4.56 or later.
Affected Software/OS Apache HTTP Server versions 2.4.0 through 2.4.55.
Vulnerability Insight Some mod_proxy configurations allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host.
... continues on next page ...

...continued from previous page...	
Details: Apache HTTP Server 2.4.0 - 2.4.55 HTTP Request Smuggling Vulnerability - Linux OID:1.3.6.1.4.1.25623.1.0.104597 Version used: 2024-02-15T05:05:40Z	
Product Detection Result Product: cpe:/a:apache:http_server:2.4.52 Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)	
References cve: CVE-2023-25690 url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.56 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2023-3129 cert-bund: WID-SEC-2023-2694 cert-bund: WID-SEC-2023-2031 cert-bund: WID-SEC-2023-1809 cert-bund: WID-SEC-2023-1807 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-1021 cert-bund: WID-SEC-2023-0657 cert-bund: WID-SEC-2023-0583 dfn-cert: DFN-CERT-2023-1648 dfn-cert: DFN-CERT-2023-1297 dfn-cert: DFN-CERT-2023-1232 dfn-cert: DFN-CERT-2023-0884 dfn-cert: DFN-CERT-2023-0788 dfn-cert: DFN-CERT-2023-0658 dfn-cert: DFN-CERT-2023-0546	

High (CVSS: 9.8) NVT: OpenBSD OpenSSH 8.9 - 9.2 Unspecified Vulnerability	
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)	
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.	
Quality of Detection (QoD): 30%	
Vulnerability Detection Result Installed version: 8.9p1	
... continues on next page ...	

...continued from previous page...	
Fixed version:	9.3
Installation path / port:	/usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.3 or later.	
Affected Software/OS OpenBSD OpenSSH versions starting from 8.9 and prior to 9.3.	
Vulnerability Insight ssh-add(1): when adding smartcard keys to ssh-agent(1) with the per-hop destination constraints (ssh-add -h ...) added in OpenSSH 8.9, a logic error prevented the constraints from being communicated to the agent. This resulted in the keys being added without constraints. The common cases of non-smartcard keys and keys without destination constraints are unaffected. This problem was reported by Luci Stanescu.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH 8.9 - 9.2 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104634 Version used: 2025-01-21T05:37:33Z	
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)	
References cve: CVE-2023-28531 url: https://www.openssh.com/releases.html#9.3 url: https://www.openwall.com/lists/oss-security/2023/03/15/8 cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2023-0670 dfn-cert: DFN-CERT-2024-1260 dfn-cert: DFN-CERT-2024-0341 dfn-cert: DFN-CERT-2023-3218 dfn-cert: DFN-CERT-2023-3182 dfn-cert: DFN-CERT-2023-1424	
High (CVSS: 9.8) NVT: OpenBSD OpenSSH 8.9 - 9.2 Unspecified Vulnerability	
Product detection result	
... continues on next page ...	

...continued from previous page ...
cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.3 Installation path / port: /snap/core22/1748/usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.3 or later.
Affected Software/OS OpenBSD OpenSSH versions starting from 8.9 and prior to 9.3.
Vulnerability Insight ssh-add(1): when adding smartcard keys to ssh-agent(1) with the per-hop destination constraints (ssh-add -h ...) added in OpenSSH 8.9, a logic error prevented the constraints from being communicated to the agent. This resulted in the keys being added without constraints. The common cases of non-smartcard keys and keys without destination constraints are unaffected. This problem was reported by Luci Stanescu.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH 8.9 - 9.2 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104634 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2023-28531 url: https://www.openssh.com/releases/notes.html#9.3 url: https://www.openwall.com/lists/oss-security/2023/03/15/8 cert-bund: WID-SEC-2024-1082
...continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2023-0670
dfn-cert: DFN-CERT-2024-1260
dfn-cert: DFN-CERT-2024-0341
dfn-cert: DFN-CERT-2023-3218
dfn-cert: DFN-CERT-2023-3182
dfn-cert: DFN-CERT-2023-1424

High (CVSS: 9.8) NVT: OpenBSD OpenSSH 8.9 - 9.2 Unspecified Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.3 Installation path / port: /snap/core22/1748/usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.3 or later.
Affected Software/OS OpenBSD OpenSSH versions starting from 8.9 and prior to 9.3.
Vulnerability Insight ssh-add(1): when adding smartcard keys to ssh-agent(1) with the per-hop destination constraints (ssh-add -h ...) added in OpenSSH 8.9, a logic error prevented the constraints from being communicated to the agent. This resulted in the keys being added without constraints. The common cases of non-smartcard keys and keys without destination constraints are unaffected. This problem was reported by Luci Stanescu.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH 8.9 - 9.2 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104634 Version used: 2025-01-21T05:37:33Z
... continues on next page ...

...continued from previous page ...
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2023-28531 url: https://www.openssh.com/releases.html#9.3 url: https://www.openwall.com/lists/oss-security/2023/03/15/8 cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2023-0670 dfn-cert: DFN-CERT-2024-1260 dfn-cert: DFN-CERT-2024-0341 dfn-cert: DFN-CERT-2023-3218 dfn-cert: DFN-CERT-2023-3182 dfn-cert: DFN-CERT-2023-1424
High (CVSS: 9.8) NVT: OpenBSD OpenSSH 8.9 - 9.2 Unspecified Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.3 Installation path / port: /snap/core22/1612/usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.3 or later.
Affected Software/OS OpenBSD OpenSSH versions starting from 8.9 and prior to 9.3.
Vulnerability Insight
... continues on next page ...

...continued from previous page ...
<p>ssh-add(1): when adding smartcard keys to ssh-agent(1) with the per-hop destination constraints (ssh-add -h ...) added in OpenSSH 8.9, a logic error prevented the constraints from being communicated to the agent. This resulted in the keys being added without constraints. The common cases of non-smartcard keys and keys without destination constraints are unaffected. This problem was reported by Luci Stanescu.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH 8.9 - 9.2 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104634 Version used: 2025-01-21T05:37:33Z</p>
<p>Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>References cve: CVE-2023-28531 url: https://www.openssh.com/releasenotes.html#9.3 url: https://www.openwall.com/lists/oss-security/2023/03/15/8 cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2023-0670 dfn-cert: DFN-CERT-2024-1260 dfn-cert: DFN-CERT-2024-0341 dfn-cert: DFN-CERT-2023-3218 dfn-cert: DFN-CERT-2023-3182 dfn-cert: DFN-CERT-2023-1424</p>
<p>High (CVSS: 9.8) NVT: OpenSSL: The c_rehash script allows command injection (CVE-2022-2068) - Linux</p>
<p>Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
<p>Summary OpenSSL is prone to a command injection vulnerability.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.4 Installation</p>
... continues on next page ...

...continued from previous page ...	
path / port:	/snap/core22/1612/usr/bin/openssl
Solution: Solution type: VendorFix Update to version 1.0.2zf, 1.1.1p, 3.0.4 or later.	
Affected Software/OS OpenSSL version 1.0.2, 1.1.1 and 3.0.	
Vulnerability Insight In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL: The c_rehash script allows command injection (CVE-2022-2068) - Linux OID:1.3.6.1.4.1.25623.1.0.148306 Version used: 2022-07-01T10:11:09Z	
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)	
References cve: CVE-2022-2068 url: https://www.openssl.org/news/secadv/20220621.txt cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-1186 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2024-0054 cert-bund: WID-SEC-2023-2723 cert-bund: WID-SEC-2023-1969 cert-bund: WID-SEC-2023-1432 cert-bund: WID-SEC-2022-1766 cert-bund: WID-SEC-2022-1461	
... continues on next page ...	

...continued from previous page ...
cert-bund: WID-SEC-2022-1245
cert-bund: WID-SEC-2022-1068
cert-bund: WID-SEC-2022-0425
dfn-cert: DFN-CERT-2024-2451
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2024-0059
dfn-cert: DFN-CERT-2023-2667
dfn-cert: DFN-CERT-2023-2600
dfn-cert: DFN-CERT-2023-2599
dfn-cert: DFN-CERT-2023-2571
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2150
dfn-cert: DFN-CERT-2022-2111
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-1905
dfn-cert: DFN-CERT-2022-1740
dfn-cert: DFN-CERT-2022-1646
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1521
dfn-cert: DFN-CERT-2022-1520
dfn-cert: DFN-CERT-2022-1425
dfn-cert: DFN-CERT-2022-1393

High (CVSS: 9.8)

NVT: OpenSSL: The c_rehash script allows command injection (CVE-2022-2068) - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to a command injection vulnerability.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 3.0.2

Fixed version: 3.0.4

Installation

path / port: /snap/core22/1748/usr/bin/openssl

Solution:

Solution type: VendorFix

Update to version 1.0.2zf, 1.1.1p, 3.0.4 or later.

... continues on next page ...

...continued from previous page ...
Affected Software/OS OpenSSL version 1.0.2, 1.1.1 and 3.0.
Vulnerability Insight In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL: The c_rehash script allows command injection (CVE-2022-2068) - Linux OID:1.3.6.1.4.1.25623.1.0.148306 Version used: 2022-07-01T10:11:09Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2022-2068 url: https://www.openssl.org/news/secadv/20220621.txt cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-1186 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2024-0054 cert-bund: WID-SEC-2023-2723 cert-bund: WID-SEC-2023-1969 cert-bund: WID-SEC-2023-1432 cert-bund: WID-SEC-2022-1766 cert-bund: WID-SEC-2022-1461 cert-bund: WID-SEC-2022-1245 cert-bund: WID-SEC-2022-1068 cert-bund: WID-SEC-2022-0425 dfn-cert: DFN-CERT-2024-2451 dfn-cert: DFN-CERT-2024-0147
...continues on next page ...

...continued from previous page ...

```

dfn-cert: DFN-CERT-2024-0059
dfn-cert: DFN-CERT-2023-2667
dfn-cert: DFN-CERT-2023-2600
dfn-cert: DFN-CERT-2023-2599
dfn-cert: DFN-CERT-2023-2571
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2150
dfn-cert: DFN-CERT-2022-2111
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-1905
dfn-cert: DFN-CERT-2022-1740
dfn-cert: DFN-CERT-2022-1646
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1521
dfn-cert: DFN-CERT-2022-1520
dfn-cert: DFN-CERT-2022-1425
dfn-cert: DFN-CERT-2022-1393

```

High (CVSS: 9.8)

NVT: OpenSSL: The c_rehash script allows command injection (CVE-2022-2068) - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to a command injection vulnerability.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 3.0.2

Fixed version: 3.0.4

Installation

path / port: /usr/bin/openssl

Solution:**Solution type:** VendorFix

Update to version 1.0.2zf, 1.1.1p, 3.0.4 or later.

Affected Software/OS

OpenSSL version 1.0.2, 1.1.1 and 3.0.

... continues on next page ...

...continued from previous page ...

Vulnerability Insight

In addition to the `c_rehash` shell command injection identified in CVE-2022-1292, further circumstances where the `c_rehash` script does not properly sanitise shell metacharacters to prevent command injection were found by code review.

When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell.

This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script.

Use of the `c_rehash` script is considered obsolete and should be replaced by the OpenSSL `rehash` command line tool.

Vulnerability Detection Method

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

Details: OpenSSL: The `c_rehash` script allows command injection (CVE-2022-2068) - Linux

OID: 1.3.6.1.4.1.25623.1.0.148306

Version used: 2022-07-01T10:11:09Z

Product Detection Result

Product: `cpe:/a:openssl:openssl:3.0.2`

Method: OpenSSL Detection Consolidation

OID: 1.3.6.1.4.1.25623.1.0.145462)

References

cve: CVE-2022-2068

url: <https://www.openssl.org/news/secadv/20220621.txt>

cert-bund: WID-SEC-2024-3195

cert-bund: WID-SEC-2024-1186

cert-bund: WID-SEC-2024-0794

cert-bund: WID-SEC-2024-0054

cert-bund: WID-SEC-2023-2723

cert-bund: WID-SEC-2023-1969

cert-bund: WID-SEC-2023-1432

cert-bund: WID-SEC-2022-1766

cert-bund: WID-SEC-2022-1461

cert-bund: WID-SEC-2022-1245

cert-bund: WID-SEC-2022-1068

cert-bund: WID-SEC-2022-0425

dfn-cert: DFN-CERT-2024-2451

dfn-cert: DFN-CERT-2024-0147

dfn-cert: DFN-CERT-2024-0059

dfn-cert: DFN-CERT-2023-2667

dfn-cert: DFN-CERT-2023-2600

dfn-cert: DFN-CERT-2023-2599

...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2023-2571
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2150
dfn-cert: DFN-CERT-2022-2111
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-1905
dfn-cert: DFN-CERT-2022-1740
dfn-cert: DFN-CERT-2022-1646
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1521
dfn-cert: DFN-CERT-2022-1520
dfn-cert: DFN-CERT-2022-1425
dfn-cert: DFN-CERT-2022-1393

High (CVSS: 9.8)

NVT: OpenSSL: Multiple Vulnerabilities (May 2022) - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 3.0.2

Fixed version: 3.0.3

Installation

path / port: /snap/core22/1612/usr/bin/openssl

Solution:

Solution type: VendorFix

Update to version 3.0.3 or later.

Affected Software/OS

OpenSSL version 3.0.x.

Vulnerability Insight

The following vulnerabilities exist:

- CVE-2022-1292: The c_rehash script allows command injection

- CVE-2022-1343: OCSP_basic_verify may incorrectly verify the response signing certificate

... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - CVE-2022-1434: Incorrect MAC key used in the RC4-MD5 ciphersuite - CVE-2022-1473: Resource leakage when decoding certificates and keys
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: <code>OpenSSL: Multiple Vulnerabilities (May 2022) - Linux</code></p> <p>OID: 1.3.6.1.4.1.25623.1.0.148047</p> <p>Version used: 2022-05-13T03:03:55Z</p>
<p>Product Detection Result</p> <p>Product: <code>cpe:/a:openssl:openssl:3.0.2</code></p> <p>Method: <code>OpenSSL Detection Consolidation</code></p> <p>OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
<p>References</p> <p>cve: CVE-2022-1292</p> <p>cve: CVE-2022-1343</p> <p>cve: CVE-2022-1434</p> <p>cve: CVE-2022-1473</p> <p>url: https://www.openssl.org/news/secadv/20220503.txt</p> <p>cert-bund: WID-SEC-2024-1186</p> <p>cert-bund: WID-SEC-2024-0794</p> <p>cert-bund: WID-SEC-2023-2723</p> <p>cert-bund: WID-SEC-2023-1432</p> <p>cert-bund: WID-SEC-2023-1424</p> <p>cert-bund: WID-SEC-2023-1021</p> <p>cert-bund: WID-SEC-2022-1775</p> <p>cert-bund: WID-SEC-2022-1767</p> <p>cert-bund: WID-SEC-2022-1461</p> <p>cert-bund: WID-SEC-2022-1245</p> <p>cert-bund: WID-SEC-2022-1068</p> <p>cert-bund: WID-SEC-2022-0833</p> <p>cert-bund: WID-SEC-2022-0826</p> <p>cert-bund: WID-SEC-2022-0755</p> <p>cert-bund: WID-SEC-2022-0735</p> <p>cert-bund: WID-SEC-2022-0555</p> <p>cert-bund: WID-SEC-2022-0393</p> <p>cert-bund: WID-SEC-2022-0071</p> <p>cert-bund: CB-K22/0536</p> <p>dfn-cert: DFN-CERT-2024-2686</p> <p>dfn-cert: DFN-CERT-2024-2451</p> <p>dfn-cert: DFN-CERT-2024-0147</p> <p>dfn-cert: DFN-CERT-2023-2667</p> <p>dfn-cert: DFN-CERT-2023-2600</p> <p>dfn-cert: DFN-CERT-2023-2599</p> <p>dfn-cert: DFN-CERT-2023-2571</p>
...continues on next page ...

...	...continued from previous page ...
dfn-cert:	DFN-CERT-2023-0372
dfn-cert:	DFN-CERT-2023-0100
dfn-cert:	DFN-CERT-2023-0081
dfn-cert:	DFN-CERT-2022-2799
dfn-cert:	DFN-CERT-2022-2323
dfn-cert:	DFN-CERT-2022-2309
dfn-cert:	DFN-CERT-2022-2150
dfn-cert:	DFN-CERT-2022-2111
dfn-cert:	DFN-CERT-2022-2073
dfn-cert:	DFN-CERT-2022-2072
dfn-cert:	DFN-CERT-2022-1905
dfn-cert:	DFN-CERT-2022-1875
dfn-cert:	DFN-CERT-2022-1837
dfn-cert:	DFN-CERT-2022-1646
dfn-cert:	DFN-CERT-2022-1609
dfn-cert:	DFN-CERT-2022-1520
dfn-cert:	DFN-CERT-2022-1425
dfn-cert:	DFN-CERT-2022-1267
dfn-cert:	DFN-CERT-2022-1103
dfn-cert:	DFN-CERT-2022-0986

High (CVSS: 9.8)

NVT: OpenSSL: Multiple Vulnerabilities (May 2022) - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 3.0.2

Fixed version: 3.0.3

Installation

path / port: /snap/core22/1748/usr/bin/openssl

Solution:

Solution type: VendorFix

Update to version 3.0.3 or later.

Affected Software/OS

... continues on next page ...

...continued from previous page ...
OpenSSL version 3.0.x.
Vulnerability Insight The following vulnerabilities exist: <ul style="list-style-type: none"> - CVE-2022-1292: The c_rehash script allows command injection - CVE-2022-1343: OCSP_basic_verify may incorrectly verify the response signing certificate - CVE-2022-1434: Incorrect MAC key used in the RC4-MD5 ciphersuite - CVE-2022-1473: Resource leakage when decoding certificates and keys
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL: Multiple Vulnerabilities (May 2022) - Linux OID: 1.3.6.1.4.1.25623.1.0.148047 Version used: 2022-05-13T03:03:55Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2022-1292 cve: CVE-2022-1343 cve: CVE-2022-1434 cve: CVE-2022-1473 url: https://www.openssl.org/news/secadv/20220503.txt cert-bund: WID-SEC-2024-1186 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2023-2723 cert-bund: WID-SEC-2023-1432 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-1021 cert-bund: WID-SEC-2022-1775 cert-bund: WID-SEC-2022-1767 cert-bund: WID-SEC-2022-1461 cert-bund: WID-SEC-2022-1245 cert-bund: WID-SEC-2022-1068 cert-bund: WID-SEC-2022-0833 cert-bund: WID-SEC-2022-0826 cert-bund: WID-SEC-2022-0755 cert-bund: WID-SEC-2022-0735 cert-bund: WID-SEC-2022-0555 cert-bund: WID-SEC-2022-0393 cert-bund: WID-SEC-2022-0071 cert-bund: CB-K22/0536 dfn-cert: DFN-CERT-2024-2686
... continues on next page ...

...continued from previous page ...

```

dfn-cert: DFN-CERT-2024-2451
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2023-2667
dfn-cert: DFN-CERT-2023-2600
dfn-cert: DFN-CERT-2023-2599
dfn-cert: DFN-CERT-2023-2571
dfn-cert: DFN-CERT-2023-0372
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2023-0081
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2309
dfn-cert: DFN-CERT-2022-2150
dfn-cert: DFN-CERT-2022-2111
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-1905
dfn-cert: DFN-CERT-2022-1875
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1646
dfn-cert: DFN-CERT-2022-1609
dfn-cert: DFN-CERT-2022-1520
dfn-cert: DFN-CERT-2022-1425
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1103
dfn-cert: DFN-CERT-2022-0986

```

High (CVSS: 9.8)

NVT: OpenSSL: Multiple Vulnerabilities (May 2022) - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 3.0.2

Fixed version: 3.0.3

Installation

path / port: /usr/bin/openssl

Solution:

... continues on next page ...

...continued from previous page...	
Solution type: VendorFix	Update to version 3.0.3 or later.
Affected Software/OS	OpenSSL version 3.0.x.
Vulnerability Insight	<p>The following vulnerabilities exist:</p> <ul style="list-style-type: none"> - CVE-2022-1292: The c_rehash script allows command injection - CVE-2022-1343: OCSP_basic_verify may incorrectly verify the response signing certificate - CVE-2022-1434: Incorrect MAC key used in the RC4-MD5 ciphersuite - CVE-2022-1473: Resource leakage when decoding certificates and keys
Vulnerability Detection Method	<p>Checks if a vulnerable version is present on the target host.</p> <p>Details: <code>OpenSSL: Multiple Vulnerabilities (May 2022) - Linux</code></p> <p>OID: 1.3.6.1.4.1.25623.1.0.148047</p> <p>Version used: 2022-05-13T03:03:55Z</p>
Product Detection Result	<p>Product: <code>cpe:/a:openssl:openssl:3.0.2</code></p> <p>Method: <code>OpenSSL Detection Consolidation</code></p> <p>OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
References	<p>cve: CVE-2022-1292</p> <p>cve: CVE-2022-1343</p> <p>cve: CVE-2022-1434</p> <p>cve: CVE-2022-1473</p> <p>url: https://www.openssl.org/news/secadv/20220503.txt</p> <p>cert-bund: WID-SEC-2024-1186</p> <p>cert-bund: WID-SEC-2024-0794</p> <p>cert-bund: WID-SEC-2023-2723</p> <p>cert-bund: WID-SEC-2023-1432</p> <p>cert-bund: WID-SEC-2023-1424</p> <p>cert-bund: WID-SEC-2023-1021</p> <p>cert-bund: WID-SEC-2022-1775</p> <p>cert-bund: WID-SEC-2022-1767</p> <p>cert-bund: WID-SEC-2022-1461</p> <p>cert-bund: WID-SEC-2022-1245</p> <p>cert-bund: WID-SEC-2022-1068</p> <p>cert-bund: WID-SEC-2022-0833</p> <p>cert-bund: WID-SEC-2022-0826</p> <p>cert-bund: WID-SEC-2022-0755</p> <p>cert-bund: WID-SEC-2022-0735</p>
...continues on next page...	

...continued from previous page ...
cert-bund: WID-SEC-2022-0555 cert-bund: WID-SEC-2022-0393 cert-bund: WID-SEC-2022-0071 cert-bund: CB-K22/0536 dfn-cert: DFN-CERT-2024-2686 dfn-cert: DFN-CERT-2024-2451 dfn-cert: DFN-CERT-2024-0147 dfn-cert: DFN-CERT-2023-2667 dfn-cert: DFN-CERT-2023-2600 dfn-cert: DFN-CERT-2023-2599 dfn-cert: DFN-CERT-2023-2571 dfn-cert: DFN-CERT-2023-0372 dfn-cert: DFN-CERT-2023-0100 dfn-cert: DFN-CERT-2023-0081 dfn-cert: DFN-CERT-2022-2799 dfn-cert: DFN-CERT-2022-2323 dfn-cert: DFN-CERT-2022-2309 dfn-cert: DFN-CERT-2022-2150 dfn-cert: DFN-CERT-2022-2111 dfn-cert: DFN-CERT-2022-2073 dfn-cert: DFN-CERT-2022-2072 dfn-cert: DFN-CERT-2022-1905 dfn-cert: DFN-CERT-2022-1875 dfn-cert: DFN-CERT-2022-1837 dfn-cert: DFN-CERT-2022-1646 dfn-cert: DFN-CERT-2022-1609 dfn-cert: DFN-CERT-2022-1520 dfn-cert: DFN-CERT-2022-1425 dfn-cert: DFN-CERT-2022-1267 dfn-cert: DFN-CERT-2022-1103 dfn-cert: DFN-CERT-2022-0986

High (CVSS: 9.8)
NVT: OpenBSD OpenSSH < 9.3p2 RCE Vulnerability

Product detection result

cpe:/a:openbsd:openssh:8.9p1

Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

Summary

OpenBSD OpenSSH is prone to a remote code execution (RCE) vulnerability in OpenSSH's forwarded ssh-agent.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

... continues on next page ...

...continued from previous page ...
<p>Installed version: 8.9p1 Fixed version: 9.3p2 Installation path / port: /snap/core22/1612/usr/bin/ssh</p>
<p>Solution: Solution type: VendorFix Update to version 9.3p2 or later.</p>
<p>Affected Software/OS OpenBSD OpenSSH prior to version 9.3p2. The following conditions needs to be met: - Exploitation requires the presence of specific libraries on the victim system. - Remote exploitation requires that the agent was forwarded to an attacker-controlled system.</p>
<p>Vulnerability Insight A condition where specific libraries loaded via ssh-agent(1)'s PKCS#11 support could be abused to achieve remote code execution via a forwarded agent socket.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.3p2 RCE Vulnerability OID:1.3.6.1.4.1.25623.1.0.104869 Version used: 2023-10-13T05:06:10Z</p>
<p>Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>References cve: CVE-2023-38408 url: https://www.openssh.com/releases.html#9.3p2 url: https://www.qualys.com/2023/07/19/cve-2023-38408/rce-openssh-forwarded-ssh-agent.txt cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2023-2679 cert-bund: WID-SEC-2023-2625 cert-bund: WID-SEC-2023-2240 cert-bund: WID-SEC-2023-1843 cert-bund: WID-SEC-2023-1819 dfn-cert: DFN-CERT-2024-1260</p>
... continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2023-2792
dfn-cert: DFN-CERT-2023-2179
dfn-cert: DFN-CERT-2023-1961
dfn-cert: DFN-CERT-2023-1920
dfn-cert: DFN-CERT-2023-1845
dfn-cert: DFN-CERT-2023-1773
dfn-cert: DFN-CERT-2023-1665

High (CVSS: 9.8) NVT: OpenBSD OpenSSH < 9.3p2 RCE Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to a remote code execution (RCE) vulnerability in OpenSSH's forwarded ssh-agent.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.3p2 Installation path / port: /snap/core22/1612/usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.3p2 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.3p2. The following conditions needs to be met: - Exploitation requires the presence of specific libraries on the victim system. - Remote exploitation requires that the agent was forwarded to an attacker-controlled system.
Vulnerability Insight A condition where specific libraries loaded via ssh-agent(1)'s PKCS#11 support could be abused to achieve remote code execution via a forwarded agent socket.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host.
... continues on next page ...

...continued from previous page ...
Details: OpenBSD OpenSSH < 9.3p2 RCE Vulnerability OID:1.3.6.1.4.1.25623.1.0.104869 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2023-38408 url: https://www.openssh.com/releasesnotes.html#9.3p2 url: https://www.qualys.com/2023/07/19/cve-2023-38408/rce-openssh-forwarded-ssh-agent.txt cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2023-2679 cert-bund: WID-SEC-2023-2625 cert-bund: WID-SEC-2023-2240 cert-bund: WID-SEC-2023-1843 cert-bund: WID-SEC-2023-1819 dfn-cert: DFN-CERT-2024-1260 dfn-cert: DFN-CERT-2024-0491 dfn-cert: DFN-CERT-2023-2792 dfn-cert: DFN-CERT-2023-2179 dfn-cert: DFN-CERT-2023-1961 dfn-cert: DFN-CERT-2023-1920 dfn-cert: DFN-CERT-2023-1845 dfn-cert: DFN-CERT-2023-1773 dfn-cert: DFN-CERT-2023-1665
High (CVSS: 9.8) NVT: OpenBSD OpenSSH < 9.3p2 RCE Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to a remote code execution (RCE) vulnerability in OpenSSH's forwarded ssh-agent.
... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.3p2 Installation path / port: /snap/core22/1748/usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.3p2 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.3p2. The following conditions needs to be met: - Exploitation requires the presence of specific libraries on the victim system. - Remote exploitation requires that the agent was forwarded to an attacker-controlled system.
Vulnerability Insight A condition where specific libraries loaded via ssh-agent(1)'s PKCS#11 support could be abused to achieve remote code execution via a forwarded agent socket.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.3p2 RCE Vulnerability OID:1.3.6.1.4.1.25623.1.0.104869 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2023-38408 url: https://www.openssh.com/releases.html#9.3p2 url: https://www.qualys.com/2023/07/19/cve-2023-38408/rce-openssh-forwarded-ssh-agent.txt cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2023-2679 cert-bund: WID-SEC-2023-2625 cert-bund: WID-SEC-2023-2240
... continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2023-1843
cert-bund: WID-SEC-2023-1819
dfn-cert: DFN-CERT-2024-1260
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2023-2792
dfn-cert: DFN-CERT-2023-2179
dfn-cert: DFN-CERT-2023-1961
dfn-cert: DFN-CERT-2023-1920
dfn-cert: DFN-CERT-2023-1845
dfn-cert: DFN-CERT-2023-1773
dfn-cert: DFN-CERT-2023-1665

High (CVSS: 9.8) NVT: OpenBSD OpenSSH < 9.3p2 RCE Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to a remote code execution (RCE) vulnerability in OpenSSH's forwarded ssh-agent.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.3p2 Installation path / port: /snap/core22/1748/usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.3p2 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.3p2. The following conditions needs to be met: - Exploitation requires the presence of specific libraries on the victim system. - Remote exploitation requires that the agent was forwarded to an attacker-controlled system.
Vulnerability Insight A condition where specific libraries loaded via ssh-agent(1)'s PKCS#11 support could be abused to achieve remote code execution via a forwarded agent socket.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.3p2 RCE Vulnerability OID:1.3.6.1.4.1.25623.1.0.104869 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2023-38408 url: https://www.openssh.com/releasesnotes.html#9.3p2 url: https://www.qualys.com/2023/07/19/cve-2023-38408/rce-openssh-forwarded-ssh-agent.txt cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2023-2679 cert-bund: WID-SEC-2023-2625 cert-bund: WID-SEC-2023-2240 cert-bund: WID-SEC-2023-1843 cert-bund: WID-SEC-2023-1819 dfn-cert: DFN-CERT-2024-1260 dfn-cert: DFN-CERT-2024-0491 dfn-cert: DFN-CERT-2023-2792 dfn-cert: DFN-CERT-2023-2179 dfn-cert: DFN-CERT-2023-1961 dfn-cert: DFN-CERT-2023-1920 dfn-cert: DFN-CERT-2023-1845 dfn-cert: DFN-CERT-2023-1773 dfn-cert: DFN-CERT-2023-1665
High (CVSS: 9.8) NVT: OpenBSD OpenSSH < 9.3p2 RCE Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary
... continues on next page ...

...continued from previous page ...
OpenBSD OpenSSH is prone to a remote code execution (RCE) vulnerability in OpenSSH's forwarded ssh-agent.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.3p2 Installation path / port: /usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.3p2 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.3p2. The following conditions needs to be met: - Exploitation requires the presence of specific libraries on the victim system. - Remote exploitation requires that the agent was forwarded to an attacker-controlled system.
Vulnerability Insight A condition where specific libraries loaded via ssh-agent(1)'s PKCS#11 support could be abused to achieve remote code execution via a forwarded agent socket.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.3p2 RCE Vulnerability OID:1.3.6.1.4.1.25623.1.0.104869 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2023-38408 url: https://www.openssh.com/releases/notes.html#9.3p2 url: https://www.qualys.com/2023/07/19/cve-2023-38408/rce-openssh-forwarded-ssh-agent.txt cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2024-0064
... continues on next page ...

...continued from previous page ...

cert-bund: WID-SEC-2023-2679
 cert-bund: WID-SEC-2023-2625
 cert-bund: WID-SEC-2023-2240
 cert-bund: WID-SEC-2023-1843
 cert-bund: WID-SEC-2023-1819
 dfn-cert: DFN-CERT-2024-1260
 dfn-cert: DFN-CERT-2024-0491
 dfn-cert: DFN-CERT-2023-2792
 dfn-cert: DFN-CERT-2023-2179
 dfn-cert: DFN-CERT-2023-1961
 dfn-cert: DFN-CERT-2023-1920
 dfn-cert: DFN-CERT-2023-1845
 dfn-cert: DFN-CERT-2023-1773
 dfn-cert: DFN-CERT-2023-1665

High (CVSS: 9.8)**NVT: OpenBSD OpenSSH 8.9 - 9.2 Unspecified Vulnerability****Product detection result**

cpe:/a:openbsd:openssh:8.9p1

Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

Summary

OpenBSD OpenSSH is prone to an unspecified vulnerability.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 8.9p1

Fixed version: 9.3

Installation

path / port: /usr/sbin/sshd

Solution:**Solution type:** VendorFix

Update to version 9.3 or later.

Affected Software/OS

OpenBSD OpenSSH versions starting from 8.9 and prior to 9.3.

Vulnerability Insight

... continues on next page ...

...continued from previous page ...
ssh-add(1): when adding smartcard keys to ssh-agent(1) with the per-hop destination constraints (ssh-add -h ...) added in OpenSSH 8.9, a logic error prevented the constraints from being communicated to the agent. This resulted in the keys being added without constraints. The common cases of non-smartcard keys and keys without destination constraints are unaffected. This problem was reported by Luci Stanescu.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH 8.9 - 9.2 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104634 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2023-28531 url: https://www.openssh.com/releasenotes.html#9.3 url: https://www.openwall.com/lists/oss-security/2023/03/15/8 cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2023-0670 dfn-cert: DFN-CERT-2024-1260 dfn-cert: DFN-CERT-2024-0341 dfn-cert: DFN-CERT-2023-3218 dfn-cert: DFN-CERT-2023-3182 dfn-cert: DFN-CERT-2023-1424
High (CVSS: 9.8) NVT: Mozilla Firefox Security Advisory (MFSA2024-51) - Linux
Product detection result cpe:/a:mozilla:firefox:136.0 Detected by Mozilla Firefox Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.2 ↪5623.1.0.800017)
Summary This host is missing a security update for Mozilla Firefox.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 130.0 Fixed version: 131.0.2
... continues on next page ...

...continued from previous page...	
Installation	
path / port:	/snap/firefox/4848/usr/lib/firefox/firefox
Solution:	
Solution type: VendorFix	
The vendor has released an update. Please see the reference(s) for more information.	
Affected Software/OS	
Firefox version(s) below 131.0.2.	
Vulnerability Insight	
CVE-2024-9680: Use-after-free in Animation timeline An attacker was able to achieve code execution in the content process by exploiting a use-after-free in Animation timelines. We have had reports of this vulnerability being exploited in the wild.	
Vulnerability Detection Method	
Checks if a vulnerable package version is present on the target host. Details: Mozilla Firefox Security Advisory (MFSA2024-51) - Linux OID:1.3.6.1.4.1.25623.1.2.1.2024.51 Version used: 2025-01-09T06:16:22Z	
Product Detection Result	
Product: cpe:/a:mozilla:firefox:136.0 Method: Mozilla Firefox Detection (Linux/Unix SSH Login) OID: 1.3.6.1.4.1.25623.1.0.800017)	
References	
cve: CVE-2024-9680 advisory-id: MFSA2024-51 url: https://www.mozilla.org/en-US/security/advisories/mfsa2024-51/ url: https://bugzilla.mozilla.org/show_bug.cgi?id=1923344 url: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-49039 url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog cisa: Known Exploited Vulnerability (KEV) catalog cert-bund: WID-SEC-2024-3138 dfn-cert: DFN-CERT-2025-0030 dfn-cert: DFN-CERT-2024-3152 dfn-cert: DFN-CERT-2024-2761 dfn-cert: DFN-CERT-2024-2694 dfn-cert: DFN-CERT-2024-2691 dfn-cert: DFN-CERT-2024-2675	

High (CVSS: 9.8) NVT: OpenBSD OpenSSH < 9.3p2 RCE Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to a remote code execution (RCE) vulnerability in OpenSSH's forwarded ssh-agent.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.3p2 Installation path / port: /usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.3p2 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.3p2. The following conditions needs to be met: - Exploitation requires the presence of specific libraries on the victim system. - Remote exploitation requires that the agent was forwarded to an attacker-controlled system.
Vulnerability Insight A condition where specific libraries loaded via ssh-agent(1)'s PKCS#11 support could be abused to achieve remote code execution via a forwarded agent socket.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.3p2 RCE Vulnerability OID:1.3.6.1.4.1.25623.1.0.104869 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References
... continues on next page ...

...continued from previous page ...
cve: CVE-2023-38408 url: https://www.openssh.com/releases/notes.html#9.3p2 url: https://www.qualys.com/2023/07/19/cve-2023-38408/rce-openssh-forwarded-ssh-↵agent.txt cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2023-2679 cert-bund: WID-SEC-2023-2625 cert-bund: WID-SEC-2023-2240 cert-bund: WID-SEC-2023-1843 cert-bund: WID-SEC-2023-1819 dfn-cert: DFN-CERT-2024-1260 dfn-cert: DFN-CERT-2024-0491 dfn-cert: DFN-CERT-2023-2792 dfn-cert: DFN-CERT-2023-2179 dfn-cert: DFN-CERT-2023-1961 dfn-cert: DFN-CERT-2023-1920 dfn-cert: DFN-CERT-2023-1845 dfn-cert: DFN-CERT-2023-1773 dfn-cert: DFN-CERT-2023-1665

High (CVSS: 9.8)

NVT: PHP < 7.4.33, 8.0.x < 8.0.25, 8.1.x < 8.1.12 Security Update - Linux

Product detection result

cpe:/a:php:php:7.2.34

Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

PHP is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 7.2.34

Fixed version: 7.4.33

Installation

path / port: /usr/bin/php7.2

Solution:

Solution type: VendorFix

Update to version 7.4.33, 8.0.25, 8.1.12 or later.

... continues on next page ...

...continued from previous page...

Affected Software/OS

PHP prior to version 7.4.33, version 8.0.x through 8.0.24 and 8.1.x through 8.1.11.

Vulnerability Insight

The following vulnerabilities exist:

- CVE-2022-31630: OOB read due to insufficient input validation in imageloadfont()
- CVE-2022-37454: Buffer overflow in hash_update() on long parameter

Vulnerability Detection Method

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

Details: PHP < 7.4.33, 8.0.x < 8.0.25, 8.1.x < 8.1.12 Security Update - Linux

OID:1.3.6.1.4.1.25623.1.0.148830

Version used: 2023-10-19T05:05:21Z

Product Detection Result

Product: cpe:/a:php:php:7.2.34

Method: PHP Detection (HTTP)

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

cve: CVE-2022-31630

cve: CVE-2022-37454

url: <https://www.php.net/ChangeLog-7.php#7.4.33>

url: <https://www.php.net/ChangeLog-8.php#8.0.25>

url: <https://www.php.net/ChangeLog-8.php#8.1.12>

cert-bund: WID-SEC-2023-1021

cert-bund: WID-SEC-2023-0561

cert-bund: WID-SEC-2023-0138

cert-bund: WID-SEC-2022-1934

cert-bund: WID-SEC-2022-1816

dfn-cert: DFN-CERT-2023-0552

dfn-cert: DFN-CERT-2023-0422

dfn-cert: DFN-CERT-2023-0028

dfn-cert: DFN-CERT-2022-2869

dfn-cert: DFN-CERT-2022-2793

dfn-cert: DFN-CERT-2022-2715

dfn-cert: DFN-CERT-2022-2639

dfn-cert: DFN-CERT-2022-2638

dfn-cert: DFN-CERT-2022-2598

dfn-cert: DFN-CERT-2022-2535

dfn-cert: DFN-CERT-2022-2523

dfn-cert: DFN-CERT-2022-2420

dfn-cert: DFN-CERT-2022-2380

High (CVSS: 9.8) NVT: PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP released new versions which include a security fix.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.4.28 Installation path / port: /usr/bin/php7.2
Solution: Solution type: VendorFix Update to version 7.4.28, 8.0.16, 8.1.3 or later.
Affected Software/OS PHP prior to version 7.4.28, 8.0.x through 8.0.15 and 8.1.x through 8.1.2.
Vulnerability Insight Fix #81708: UAF due to php_filter_float() failing for ints.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Linux OID:1.3.6.1.4.1.25623.1.0.147657 Version used: 2022-03-09T03:03:43Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2021-21708 url: https://www.php.net/ChangeLog-7.php#7.4.28 url: https://www.php.net/ChangeLog-8.php#8.0.16 url: https://www.php.net/ChangeLog-8.php#8.1.3 url: https://bugs.php.net/bug.php?id=81708 ... continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0280
cert-bund: CB-K22/0201
dfn-cert: DFN-CERT-2024-1062
dfn-cert: DFN-CERT-2023-1600
dfn-cert: DFN-CERT-2022-2639
dfn-cert: DFN-CERT-2022-2598
dfn-cert: DFN-CERT-2022-2500
dfn-cert: DFN-CERT-2022-2499
dfn-cert: DFN-CERT-2022-1605
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0407
dfn-cert: DFN-CERT-2022-0365

High (CVSS: 9.8)

NVT: Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux

Product detection result

cpe:/a:apache:http_server:2.4.52

Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary

Apache HTTP Server is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 2.4.52

Fixed version: 2.4.53

Installation

path / port: /usr/sbin/apache2

Solution:

Solution type: VendorFix

Update to version 2.4.53 or later.

Affected Software/OS

Apache HTTP Server version 2.4.52 and prior.

Vulnerability Insight

The following vulnerabilities exist:

... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - CVE-2022-22719: mod_lua Use of uninitialized value of in r:parsebody - CVE-2022-22720: HTTP request smuggling vulnerability - CVE-2022-22721: Possible buffer overflow with very large or unlimited LimitXMLRequestBody - CVE-2022-23943: mod_sed: Read/write beyond bounds
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux</p> <p>OID:1.3.6.1.4.1.25623.1.0.113837</p> <p>Version used: 2022-03-21T03:03:41Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:apache:http_server:2.4.52</p> <p>Method: Apache HTTP Server Detection Consolidation</p> <p>OID: 1.3.6.1.4.1.25623.1.0.117232)</p>
<p>References</p> <p>url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.53</p> <p>cve: CVE-2022-22719</p> <p>cve: CVE-2022-22720</p> <p>cve: CVE-2022-22721</p> <p>cve: CVE-2022-23943</p> <p>cert-bund: WID-SEC-2024-1591</p> <p>cert-bund: WID-SEC-2022-1772</p> <p>cert-bund: WID-SEC-2022-1335</p> <p>cert-bund: WID-SEC-2022-1228</p> <p>cert-bund: WID-SEC-2022-1161</p> <p>cert-bund: WID-SEC-2022-1057</p> <p>cert-bund: WID-SEC-2022-0898</p> <p>cert-bund: WID-SEC-2022-0799</p> <p>cert-bund: WID-SEC-2022-0755</p> <p>cert-bund: WID-SEC-2022-0646</p> <p>cert-bund: WID-SEC-2022-0432</p> <p>cert-bund: WID-SEC-2022-0302</p> <p>cert-bund: WID-SEC-2022-0290</p> <p>cert-bund: CB-K22/0619</p> <p>cert-bund: CB-K22/0306</p> <p>dfn-cert: DFN-CERT-2022-2799</p> <p>dfn-cert: DFN-CERT-2022-2509</p> <p>dfn-cert: DFN-CERT-2022-2305</p> <p>dfn-cert: DFN-CERT-2022-2167</p> <p>dfn-cert: DFN-CERT-2022-1116</p> <p>dfn-cert: DFN-CERT-2022-1115</p> <p>dfn-cert: DFN-CERT-2022-1114</p> <p>dfn-cert: DFN-CERT-2022-0899</p> <p>dfn-cert: DFN-CERT-2022-0898</p>
...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2022-0865 dfn-cert: DFN-CERT-2022-0747 dfn-cert: DFN-CERT-2022-0678 dfn-cert: DFN-CERT-2022-0582
High (CVSS: 9.8) NVT: Apache HTTP Server < 2.4.60 Multiple Vulnerabilities - Linux
Product detection result cpe:/a:apache:http_server:2.4.52 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1 ↔.0.117232)
Summary Apache HTTP Server is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 2.4.52 Fixed version: 2.4.60 Installation path / port: /usr/sbin/apache2
Solution: Solution type: VendorFix Update to version 2.4.60 or later.
Affected Software/OS Apache HTTP Server version 2.4.59 and prior.
Vulnerability Insight The following flaws exist: <ul style="list-style-type: none"> - CVE-2024-36387: Denial of Service (DoS) by Null pointer in websocket over HTTP/2 - CVE-2024-38473: Proxy encoding problem - CVE-2024-38474: Weakness with encoded question marks in backreferences - CVE-2024-38475: Weakness in mod_rewrite when first segment of substitution matches filesystem path - CVE-2024-38476: May use exploitable/malicious backend application output to run local handlers via internal redirect - CVE-2024-38477: Crash resulting in DoS in mod_proxy via a malicious request - CVE-2024-39573: mod_rewrite proxy handler substitution
Vulnerability Detection Method
... continues on next page ...

...continued from previous page...

Checks if a vulnerable version is present on the target host.
 Details: Apache HTTP Server < 2.4.60 Multiple Vulnerabilities - Linux
 OID:1.3.6.1.4.1.25623.1.0.114682
 Version used: 2024-08-22T05:05:50Z

Product Detection Result

Product: cpe:/a:apache:http_server:2.4.52
 Method: Apache HTTP Server Detection Consolidation
 OID: 1.3.6.1.4.1.25623.1.0.117232)

References

cve: CVE-2024-36387
 cve: CVE-2024-38473
 cve: CVE-2024-38474
 cve: CVE-2024-38475
 cve: CVE-2024-38476
 cve: CVE-2024-38477
 cve: CVE-2024-39573
 url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.60
 cert-bund: WID-SEC-2025-0148
 cert-bund: WID-SEC-2025-0143
 cert-bund: WID-SEC-2024-3291
 cert-bund: WID-SEC-2024-3199
 cert-bund: WID-SEC-2024-1913
 cert-bund: WID-SEC-2024-1504
 dfn-cert: DFN-CERT-2025-0170
 dfn-cert: DFN-CERT-2024-2841
 dfn-cert: DFN-CERT-2024-2787
 dfn-cert: DFN-CERT-2024-2736
 dfn-cert: DFN-CERT-2024-2342
 dfn-cert: DFN-CERT-2024-2214
 dfn-cert: DFN-CERT-2024-2201
 dfn-cert: DFN-CERT-2024-2180
 dfn-cert: DFN-CERT-2024-2110
 dfn-cert: DFN-CERT-2024-2017
 dfn-cert: DFN-CERT-2024-1963
 dfn-cert: DFN-CERT-2024-1920
 dfn-cert: DFN-CERT-2024-1919
 dfn-cert: DFN-CERT-2024-1911
 dfn-cert: DFN-CERT-2024-1907
 dfn-cert: DFN-CERT-2024-1893
 dfn-cert: DFN-CERT-2024-1816
 dfn-cert: DFN-CERT-2024-1811
 dfn-cert: DFN-CERT-2024-1784
 dfn-cert: DFN-CERT-2024-1741
 dfn-cert: DFN-CERT-2024-1699

High (CVSS: 9.8) NVT: Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Linux
Product detection result cpe:/a:apache:http_server:2.4.52 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1 ↔.0.117232)
Summary Apache HTTP Server is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 2.4.52 Fixed version: 2.4.54 Installation path / port: /usr/sbin/apache2
Solution: Solution type: VendorFix Update to version 2.4.54 or later.
Affected Software/OS Apache HTTP Server version 2.4.53 and prior.
Vulnerability Insight The following vulnerabilities exist: - CVE-2022-26377: mod_proxy_ajp: Possible request smuggling - CVE-2022-28614: Read beyond bounds via ap_rwrite() - CVE-2022-28615: Read beyond bounds in ap_strcmp_match() - CVE-2022-29404: Denial of service in mod_lua r:parsebody - CVE-2022-30556: Information disclosure in mod_lua with websockets - CVE-2022-31813: mod_proxy X-Forwarded-For dropped by hop-by-hop mechanism
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Linux OID:1.3.6.1.4.1.25623.1.0.148252 Version used: 2022-06-20T03:04:15Z
Product Detection Result Product: cpe:/a:apache:http_server:2.4.52 Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)
... continues on next page ...

...continued from previous page ...

References

cve: CVE-2022-26377
 cve: CVE-2022-28614
 cve: CVE-2022-28615
 cve: CVE-2022-29404
 cve: CVE-2022-30556
 cve: CVE-2022-31813
 url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.54
 cert-bund: WID-SEC-2024-1591
 cert-bund: WID-SEC-2023-1969
 cert-bund: WID-SEC-2023-0134
 cert-bund: WID-SEC-2023-0132
 cert-bund: WID-SEC-2022-1767
 cert-bund: WID-SEC-2022-1766
 cert-bund: WID-SEC-2022-1764
 cert-bund: WID-SEC-2022-0858
 cert-bund: WID-SEC-2022-0192
 cert-bund: CB-K22/0692
 dfn-cert: DFN-CERT-2023-0119
 dfn-cert: DFN-CERT-2022-2799
 dfn-cert: DFN-CERT-2022-2789
 dfn-cert: DFN-CERT-2022-2652
 dfn-cert: DFN-CERT-2022-2509
 dfn-cert: DFN-CERT-2022-2310
 dfn-cert: DFN-CERT-2022-2167
 dfn-cert: DFN-CERT-2022-1837
 dfn-cert: DFN-CERT-2022-1833
 dfn-cert: DFN-CERT-2022-1720
 dfn-cert: DFN-CERT-2022-1353
 dfn-cert: DFN-CERT-2022-1296

High (CVSS: 9.8)

NVT: PHP < 8.1.31, 8.2.x < 8.2.26, 8.3.x < 8.3.14 Multiple Vulnerabilities - Linux

Product detection result

cpe:/a:php:php:7.2.34

Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

PHP is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 7.2.34

... continues on next page ...

...continued from previous page ...	
Fixed version:	8.1.31
Installation path / port:	/usr/bin/php7.2
Solution: Solution type: VendorFix Update to version 8.1.31, 8.2.26, 8.3.14 or later.	
Affected Software/OS PHP versions prior to 8.1.31, 8.2.x prior to 8.2.26 and 8.3.x prior to 8.3.14.	
Vulnerability Insight The following vulnerabilities exist: <ul style="list-style-type: none"> - CVE-2024-8929: Leak partial content of the heap through heap buffer over-read - CVE-2024-8932: OOB access in ldap_escape - CVE-2024-11233: Single byte overread with convert.quoted-printable-decode filter - CVE-2024-11234: Configuring a proxy in a stream context might allow for CRLF injection in URIs - CVE-2024-11236: Integer overflow in the firebird/dblib quoter causing OOB writes - No CVE: Heap-Use-After-Free in sapi_read_post_data Processing in CLI SAPI Interface 	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 8.1.31, 8.2.x < 8.2.26, 8.3.x < 8.3.14 Multiple Vulnerabilities - Linux OID: 1.3.6.1.4.1.25623.1.0.153495 Version used: 2025-01-13T08:32:03Z	
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)	
References cve: CVE-2024-8929 cve: CVE-2024-8932 cve: CVE-2024-11233 cve: CVE-2024-11234 cve: CVE-2024-11236 url: https://www.php.net/ChangeLog-8.php#8.1.31 url: https://www.php.net/ChangeLog-8.php#8.2.26 url: https://www.php.net/ChangeLog-8.php#8.3.14 url: https://github.com/php/php-src/security/advisories/GHSA-h35g-vwh6-m678 url: https://github.com/php/php-src/security/advisories/GHSA-g665-fm4p-vhff url: https://github.com/php/php-src/security/advisories/GHSA-r977-prxv-hc43 url: https://github.com/php/php-src/security/advisories/GHSA-c5f2-jwm7-mmq2	
... continues on next page ...	

...continued from previous page ...
url: https://github.com/php/php-src/security/advisories/GHSA-5hqh-c84r-qjcv
url: https://github.com/php/php-src/security/advisories/GHSA-4w77-75f9-2c8w
cert-bund: WID-SEC-2024-3519
dfn-cert: DFN-CERT-2025-0179
dfn-cert: DFN-CERT-2024-3200
dfn-cert: DFN-CERT-2024-3172
dfn-cert: DFN-CERT-2024-3108

High (CVSS: 9.8) NVT: PHP < 8.1.29, 8.2.x < 8.2.20, 8.3.x < 8.3.8 Multiple Vulnerabilities - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 8.1.29 Installation path / port: /usr/bin/php7.2
Solution: Solution type: VendorFix Update to version 8.1.29, 8.2.20, 8.3.8 or later.
Affected Software/OS PHP prior to version 8.1.29, version 8.2.x through 8.2.19 and 8.3.x through 8.3.7.
Vulnerability Insight The following vulnerabilities exist: - CVE-2024-4577: Argument injection in PHP-CGI (bypass of CVE-2012-1823) - CVE-2024-5458: Filter bypass in filter_var FILTER_VALIDATE_URL - CVE-2024-5585: Bypass of CVE-2024-1874 Note: As of 06/2024 the CVEs CVE-2024-4577 and CVE-2024-5585 are known to be exploitable on Windows systems only.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 8.1.29, 8.2.x < 8.2.20, 8.3.x < 8.3.8 Multiple Vulnerabilities - Linux ... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.152369 Version used: 2024-08-09T05:05:42Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2024-4577 cve: CVE-2024-5458 cve: CVE-2024-5585 cisa: Known Exploited Vulnerability (KEV) catalog url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog url: https://www.php.net/ChangeLog-8.php#8.1.29 url: https://www.php.net/ChangeLog-8.php#8.2.20 url: https://www.php.net/ChangeLog-8.php#8.3.8 url: https://github.com/php/php-src/security/advisories/GHSA-9fcc-425m-g385 url: https://github.com/php/php-src/security/advisories/GHSA-w8qr-v226-r27w url: https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability-en/ url: https://blog.orange.tw/2024/06/cve-2024-4577-yet-another-php-rce.html url: https://labs.watchtowr.com/no-way-php-strikes-again-cve-2024-4577/ url: https://github.com/watchtowrlabs/CVE-2024-4577 cert-bund: WID-SEC-2024-3196 cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-1320 dfn-cert: DFN-CERT-2024-3330 dfn-cert: DFN-CERT-2024-3329 dfn-cert: DFN-CERT-2024-2707 dfn-cert: DFN-CERT-2024-1853 dfn-cert: DFN-CERT-2024-1586 dfn-cert: DFN-CERT-2024-1574 dfn-cert: DFN-CERT-2024-1563 dfn-cert: DFN-CERT-2024-1476
High (CVSS: 9.8) NVT: PHP < 8.0.30, 8.1.x < 8.1.22, 8.2.x < 8.2.9 Security Update - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary ... continues on next page ...

...continued from previous page ...
PHP is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 8.0.30 Installation path / port: /usr/bin/php7.2
Solution: Solution type: VendorFix Update to version 8.0.30, 8.1.22, 8.2.9 or later.
Affected Software/OS PHP prior to version 8.0.30, 8.1.x prior to 8.1.22 and 8.2.x prior to 8.2.9.
Vulnerability Insight The following flaws exist: - CVE-2023-3823: Fixed bug GHSA-3qrf-m4j2-pcrr (Security issue with external entity loading in XML without enabling it) - CVE-2023-3824: Fixed bug GHSA-jqcx-ccgc-xwhv (Buffer mismanagement in phar_dir_read())
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 8.0.30, 8.1.x < 8.1.22, 8.2.x < 8.2.9 Security Update - Linux OID:1.3.6.1.4.1.25623.1.0.170529 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2023-3823 cve: CVE-2023-3824 url: https://www.php.net/ChangeLog-8.php#8.1.22 url: https://www.php.net/ChangeLog-8.php#8.0.30 url: https://www.php.net/ChangeLog-8.php#8.2.9 url: https://github.com/php/php-src/security/advisories/GHSA-3qrf-m4j2-pcrr url: https://github.com/php/php-src/security/advisories/GHSA-jqcx-ccgc-xwhv cert-bund: WID-SEC-2023-2917 cert-bund: WID-SEC-2023-2679
... continues on next page ...

...continued from previous page ...

cert-bund: WID-SEC-2023-1970
 dfn-cert: DFN-CERT-2024-3330
 dfn-cert: DFN-CERT-2024-2681
 dfn-cert: DFN-CERT-2024-0993
 dfn-cert: DFN-CERT-2023-2570
 dfn-cert: DFN-CERT-2023-2542
 dfn-cert: DFN-CERT-2023-1775

High (CVSS: 9.0)**NVT: Apache HTTP Server < 2.4.55 Multiple Vulnerabilities - Linux****Product detection result**

cpe:/a:apache:http_server:2.4.52

Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
 ↪.0.117232)

Summary

Apache HTTP Server is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 2.4.52

Fixed version: 2.4.55

Installation

path / port: /usr/sbin/apache2

Solution:**Solution type:** VendorFix

Update to version 2.4.55 or later.

Affected Software/OS

Apache HTTP Server version 2.4.54 and prior.

Vulnerability Insight

The following vulnerabilities exist:

- CVE-2006-20001: mod_dav out of bounds read, or write of zero byte
- CVE-2022-36760: Possible request smuggling in mod_proxy_ajp
- CVE-2022-37436: mod_proxy allows a backend to trigger HTTP response splitting

Vulnerability Detection Method

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

Details: Apache HTTP Server < 2.4.55 Multiple Vulnerabilities - Linux

OID:1.3.6.1.4.1.25623.1.0.149152

... continues on next page ...

...continued from previous page ...
Version used: 2024-02-15T05:05:40Z
Product Detection Result Product: cpe:/a:apache:http_server:2.4.52 Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)
References cve: CVE-2006-20001 cve: CVE-2022-36760 cve: CVE-2022-37436 url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.55 cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2023-2674 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-1022 cert-bund: WID-SEC-2023-0561 cert-bund: WID-SEC-2023-0110 dfn-cert: DFN-CERT-2023-2545 dfn-cert: DFN-CERT-2023-1895 dfn-cert: DFN-CERT-2023-1297 dfn-cert: DFN-CERT-2023-0658 dfn-cert: DFN-CERT-2023-0548 dfn-cert: DFN-CERT-2023-0497 dfn-cert: DFN-CERT-2023-0118

High (CVSS: 8.8) NVT: Mozilla Firefox Security Advisory (MFSA2024-55) - Linux
Product detection result cpe:/a:mozilla:firefox:136.0 Detected by Mozilla Firefox Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.2 ↪5623.1.0.800017)
Summary This host is missing a security update for Mozilla Firefox.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 130.0 Fixed version: 132 Installation
... continues on next page ...

...continued from previous page ...	
path / port:	/snap/firefox/4848/usr/lib/firefox/firefox
Solution: Solution type: VendorFix The vendor has released an update. Please see the reference(s) for more information.	
Affected Software/OS Firefox version(s) below 132.	
Vulnerability Insight CVE-2024-10458: Permission leak via embed or object elements A permission leak could have occurred from a trusted site to an untrusted site via embed or object elements. CVE-2024-10459: Use-after-free in layout with accessibility An attacker could have caused a use-after-free when accessibility was enabled, leading to a potentially exploitable crash. CVE-2024-10460: Confusing display of origin for external protocol handler prompt The origin of an external protocol handler prompt could have been obscured using a data: URL within an iframe. CVE-2024-10461: XSS due to Content-Disposition being ignored in multipart/x-mixed-replace response In multipart/x-mixed-replace responses, Content-Disposition: attachment in the response header was not respected and did not force a download, which could allow XSS attacks. CVE-2024-10462: Origin of permission prompt could be spoofed by long URL Truncation of a long URL could have allowed origin spoofing in a permission prompt. CVE-2024-10463: Cross origin video frame leak Video frames could have been leaked between origins in some situations. CVE-2024-10468: Race conditions in IndexedDB Potential race conditions in IndexedDB could have caused memory corruption, leading to a potentially exploitable crash. CVE-2024-10464: History interface could have been used to cause a Denial of Service condition in the browser Repeated writes to history interface attributes could have been used to cause a Denial of Service condition in the browser. This was addressed by introducing rate-limiting to this API. CVE-2024-10465: Clipboard 'paste' button persisted across tabs A clipboard 'paste' button could persist across tabs which allowed a spoofing attack. CVE-2024-10466: DOM push subscription message could hang Firefox By sending a specially crafted push message, a remote server could have hung the parent process, causing the browser to become unresponsive. CVE-2024-10467: Memory safety bugs fixed in Firefox 132, Thunderbird 132, Firefox ESR 128.4, and Thunderbird 128.4 Memory safety bugs present in Firefox 131, Firefox ESR 128.3, and Thunderbird 128.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code.	
Vulnerability Detection Method Checks if a vulnerable package version is present on the target host. Details: Mozilla Firefox Security Advisory (MFSA2024-55) - Linux OID:1.3.6.1.4.1.25623.1.2.1.2024.55 Version used: 2024-11-06T05:05:44Z	
... continues on next page ...	

...continued from previous page...

Product Detection Result

Product: cpe:/a:mozilla:firefox:136.0

Method: Mozilla Firefox Detection (Linux/Unix SSH Login)

OID: 1.3.6.1.4.1.25623.1.0.800017)

References

cve: CVE-2024-10458

cve: CVE-2024-10459

cve: CVE-2024-10460

cve: CVE-2024-10461

cve: CVE-2024-10462

cve: CVE-2024-10463

cve: CVE-2024-10464

cve: CVE-2024-10465

cve: CVE-2024-10466

cve: CVE-2024-10467

cve: CVE-2024-10468

advisory-id: MFSA2024-55

url: <https://www.mozilla.org/en-US/security/advisories/mfsa2024-55/>url: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1829029%2C1888538%2C1900394%2C1904059%2C1917742%2C1919809%2C1923706url: https://bugzilla.mozilla.org/show_bug.cgi?id=1912537url: https://bugzilla.mozilla.org/show_bug.cgi?id=1913000url: https://bugzilla.mozilla.org/show_bug.cgi?id=1914521url: https://bugzilla.mozilla.org/show_bug.cgi?id=1914982url: https://bugzilla.mozilla.org/show_bug.cgi?id=1918853url: https://bugzilla.mozilla.org/show_bug.cgi?id=1919087url: https://bugzilla.mozilla.org/show_bug.cgi?id=1920423url: https://bugzilla.mozilla.org/show_bug.cgi?id=1920800url: https://bugzilla.mozilla.org/show_bug.cgi?id=1921733url: https://bugzilla.mozilla.org/show_bug.cgi?id=1924154

cert-bund: WID-SEC-2024-3296

dfn-cert: DFN-CERT-2025-0030

dfn-cert: DFN-CERT-2024-3130

dfn-cert: DFN-CERT-2024-2852

dfn-cert: DFN-CERT-2024-2851

High (CVSS: 8.8)

NVT: PHP < 7.4.30, 8.0.x < 8.0.20, 8.1.x < 8.1.7 Security Update (Jun 2022) - Linux

Product detection result

cpe:/a:php:php:7.2.34

Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

... continues on next page ...

...continued from previous page ...
PHP released new versions which include a security fix.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.4.30 Installation path / port: /usr/bin/php7.2
Solution: Solution type: VendorFix Update to version 7.4.30, 8.0.20, 8.1.7 or later.
Affected Software/OS PHP prior to version 7.4.30, 8.0.x through 8.0.19 and 8.1.x through 8.1.6.
Vulnerability Insight The following vulnerabilities exist: - CVE-2022-31625: Uninitialized array in pg_query_params() - CVE-2022-31626: mysqlnd/pdo password buffer overflow
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.4.30, 8.0.x < 8.0.20, 8.1.x < 8.1.7 Security Update (Jun 2022) - Linux OID:1.3.6.1.4.1.25623.1.0.148249 Version used: 2023-10-19T05:05:21Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2022-31625 cve: CVE-2022-31626 url: https://www.php.net/ChangeLog-7.php#7.4.30 url: https://www.php.net/ChangeLog-8.php#8.0.20 url: https://www.php.net/ChangeLog-8.php#8.1.7 url: https://bugs.php.net/bug.php?id=81720 url: https://bugs.php.net/bug.php?id=81719 cert-bund: WID-SEC-2023-1737 cert-bund: WID-SEC-2022-0255 cert-bund: CB-K22/0700 dfn-cert: DFN-CERT-2023-1600
... continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2022-2869
dfn-cert: DFN-CERT-2022-2639
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2022-2598
dfn-cert: DFN-CERT-2022-2500
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-1881
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1516
dfn-cert: DFN-CERT-2022-1493
dfn-cert: DFN-CERT-2022-1473
dfn-cert: DFN-CERT-2022-1288

High (CVSS: 8.8) NVT: PHP < 8.1.30, 8.2.x < 8.2.24, 8.3.x < 8.3.12 Multiple Vulnerabilities - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 8.1.30 Installation path / port: /usr/bin/php7.2
Solution: Solution type: VendorFix Update to version 8.1.30, 8.2.24, 8.3.12 or later.
Affected Software/OS PHP versions prior to 8.1.30, 8.2.x prior to 8.2.24 and 8.3.x prior to 8.3.12.
Vulnerability Insight The following vulnerabilities exist: - CVE-2024-8925, CVE-2024-8928: Erroneous parsing of multipart form data - CVE-2024-8926: Bypass of CVE-2024-4577, Parameter Injection Vulnerability - CVE-2024-8927: cgi.force_redirect configuration is bypassable due to the environment variable collision
... continues on next page ...

...continued from previous page ...
- CVE-2024-9026: Logs from children may be altered
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 8.1.30, 8.2.x < 8.2.24, 8.3.x < 8.3.12 Multiple Vulnerabilities - Linux OID:1.3.6.1.4.1.25623.1.0.114787 Version used: 2024-10-17T08:02:35Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2024-8925 cve: CVE-2024-8926 cve: CVE-2024-8927 cve: CVE-2024-8928 cve: CVE-2024-9026 url: https://www.php.net/ChangeLog-8.php#8.1.30 url: https://www.php.net/ChangeLog-8.php#8.2.24 url: https://www.php.net/ChangeLog-8.php#8.3.12 url: https://github.com/php/php-src/security/advisories/GHSA-9pqp-7h25-4f32 url: https://github.com/php/php-src/security/advisories/GHSA-p99j-rfp4-xqvq url: https://github.com/php/php-src/security/advisories/GHSA-94p6-54jq-9mwp url: https://github.com/php/php-src/security/advisories/GHSA-865w-9rf3-2wh5 url: https://bugzilla.redhat.com/show_bug.cgi?id=2317439 cert-bund: WID-SEC-2025-0137 cert-bund: WID-SEC-2024-3116 cert-bund: WID-SEC-2024-2230 dfn-cert: DFN-CERT-2025-0168 dfn-cert: DFN-CERT-2024-3330 dfn-cert: DFN-CERT-2024-3329 dfn-cert: DFN-CERT-2024-2707 dfn-cert: DFN-CERT-2024-2591 dfn-cert: DFN-CERT-2024-2550
High (CVSS: 8.1) NVT: OpenBSD OpenSSH < 4.4p1, 8.5p1 - 9.7p1 RCE Vulnerability (regreSSHion)
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary
... continues on next page ...

...continued from previous page ...
OpenBSD OpenSSH is prone to a remote code execution (RCE) vulnerability dubbed 'regreSSHion'.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.8 Installation path / port: /snap/core22/1612/usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.8 or later.
Affected Software/OS OpenBSD OpenSSH versions prior to 4.4p1 (unless patched for CVE-2006-5051 and CVE-2008-4109) and 8.5p1 through 9.7p1.
Vulnerability Insight Vendor insights: 1) Race condition in sshd(8) A critical vulnerability in sshd(8) was present that may allow arbitrary code execution with root privileges. Successful exploitation has been demonstrated on 32-bit Linux/glibc systems with ASLR. Under lab conditions, the attack requires on average 6-8 hours of continuous connections up to the maximum the server will accept. Exploitation on 64-bit systems is believed to be possible but has not been demonstrated at this time. It's likely that these attacks will be improved upon. Exploitation on non-glibc systems is conceivable but has not been examined. Systems that lack ASLR or users of downstream Linux distributions that have modified OpenSSH to disable per-connection ASLR re-randomisation (yes - this is a thing, no - we don't understand why) may potentially have an easier path to exploitation. OpenBSD is not vulnerable.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 4.4p1, 8.5p1 - 9.7p1 RCE Vulnerability (regreSSHion) OID:1.3.6.1.4.1.25623.1.0.114680 Version used: 2024-07-09T05:05:54Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
... continues on next page ...

...continued from previous page ...
References cve: CVE-2024-6387 url: https://www.openssh.com/txt/release-9.8 url: https://www.openssh.com/security.html url: https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt url: https://www.qualys.com/regresshion-cve-2024-6387/ url: https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server url: https://unit42.paloaltonetworks.com/threat-brief-cve-2024-6387-openssh/ cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-1725 cert-bund: WID-SEC-2024-1486 dfn-cert: DFN-CERT-2025-0042 dfn-cert: DFN-CERT-2024-1960 dfn-cert: DFN-CERT-2024-1959 dfn-cert: DFN-CERT-2024-1958 dfn-cert: DFN-CERT-2024-1904 dfn-cert: DFN-CERT-2024-1869 dfn-cert: DFN-CERT-2024-1868 dfn-cert: DFN-CERT-2024-1844 dfn-cert: DFN-CERT-2024-1759 dfn-cert: DFN-CERT-2024-1740 dfn-cert: DFN-CERT-2024-1694 dfn-cert: DFN-CERT-2024-1693

High (CVSS: 8.1) NVT: OpenBSD OpenSSH < 4.4p1, 8.5p1 - 9.7p1 RCE Vulnerability (regreSSHion)
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to a remote code execution (RCE) vulnerability dubbed 'regreSSH-ion'.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.8 Installation path / port: /snap/core22/1612/usr/bin/ssh
Solution: Solution type: VendorFix
... continues on next page ...

...continued from previous page ...
Update to version 9.8 or later.
Affected Software/OS OpenBSD OpenSSH versions prior to 4.4p1 (unless patched for CVE-2006-5051 and CVE-2008-4109) and 8.5p1 through 9.7p1.
Vulnerability Insight Vendor insights: 1) Race condition in sshd(8) A critical vulnerability in sshd(8) was present that may allow arbitrary code execution with root privileges. Successful exploitation has been demonstrated on 32-bit Linux/glibc systems with ASLR. Under lab conditions, the attack requires on average 6-8 hours of continuous connections up to the maximum the server will accept. Exploitation on 64-bit systems is believed to be possible but has not been demonstrated at this time. It's likely that these attacks will be improved upon. Exploitation on non-glibc systems is conceivable but has not been examined. Systems that lack ASLR or users of downstream Linux distributions that have modified OpenSSH to disable per-connection ASLR re-randomisation (yes - this is a thing, no - we don't understand why) may potentially have an easier path to exploitation. OpenBSD is not vulnerable.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 4.4p1, 8.5p1 - 9.7p1 RCE Vulnerability (regreSSHion) OID:1.3.6.1.4.1.25623.1.0.114680 Version used: 2024-07-09T05:05:54Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2024-6387 url: https://www.openssh.com/txt/release-9.8 url: https://www.openssh.com/security.html url: https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt url: https://www.qualys.com/regresshion-cve-2024-6387/ url: https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server url: https://unit42.paloaltonetworks.com/threat-brief-cve-2024-6387-openssh/cert-bund cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-1725 cert-bund: WID-SEC-2024-1486 dfn-cert: DFN-CERT-2025-0042
... continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2024-1960 dfn-cert: DFN-CERT-2024-1959 dfn-cert: DFN-CERT-2024-1958 dfn-cert: DFN-CERT-2024-1904 dfn-cert: DFN-CERT-2024-1869 dfn-cert: DFN-CERT-2024-1868 dfn-cert: DFN-CERT-2024-1844 dfn-cert: DFN-CERT-2024-1759 dfn-cert: DFN-CERT-2024-1740 dfn-cert: DFN-CERT-2024-1694 dfn-cert: DFN-CERT-2024-1693
High (CVSS: 8.1) NVT: PHP < 8.0.28, 8.1.x < 8.1.16, 8.2.x < 8.2.3 Security Update - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 8.0.28 Installation path / port: /usr/bin/php7.2
Solution: Solution type: VendorFix Update to version 8.0.28, 8.1.16, 8.2.3 or later.
Affected Software/OS PHP versions prior to 8.0.28, 8.1.x prior to 8.1.16 and 8.2.x prior to 8.2.3.
Vulnerability Insight The following flaws exist: - CVE-2023-0567: Fixed bug #81744 (Password_verify() always return true with some hash) - CVE-2023-0568: Fixed bug #81746 (1-byte array overrun in common path resolve code) - CVE-2023-0662: Fixed bug GHSA-54hq-v5wp-fqgv (DOS vulnerability when parsing multipart request body)
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 8.0.28, 8.1.x < 8.1.16, 8.2.x < 8.2.3 Security Update - Linux OID:1.3.6.1.4.1.25623.1.0.104541 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2023-0567 cve: CVE-2023-0568 cve: CVE-2023-0662 url: https://www.php.net/ChangeLog-8.php#8.2.3 url: https://www.php.net/ChangeLog-8.php#8.1.16 url: https://www.php.net/ChangeLog-8.php#8.0.28 url: https://www.php.net/archive/2023.php#2023-02-14-2 url: https://www.php.net/archive/2023.php#2023-02-14-3 url: https://www.php.net/archive/2023.php#2023-02-14-1 url: http://bugs.php.net/81744 url: http://bugs.php.net/81746 url: https://github.com/php/php-src/security/advisories/GHSA-54hq-v5wp-fqgv url: https://github.com/php/php-src/security/advisories/GHSA-7fj2-8x79-rj4 cert-bund: WID-SEC-2023-2671 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-1022 cert-bund: WID-SEC-2023-0383 dfn-cert: DFN-CERT-2024-3330 dfn-cert: DFN-CERT-2024-2681 dfn-cert: DFN-CERT-2023-2570 dfn-cert: DFN-CERT-2023-2538 dfn-cert: DFN-CERT-2023-0994 dfn-cert: DFN-CERT-2023-0884 dfn-cert: DFN-CERT-2023-0462 dfn-cert: DFN-CERT-2023-0435 dfn-cert: DFN-CERT-2023-0336
High (CVSS: 8.1) NVT: OpenBSD OpenSSH < 4.4p1, 8.5p1 - 9.7p1 RCE Vulnerability (regreSSHion)
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
...continues on next page ...

...continued from previous page ...
Summary OpenBSD OpenSSH is prone to a remote code execution (RCE) vulnerability dubbed 'regreSSH-ion'.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.8 Installation path / port: /snap/core22/1748/usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.8 or later.
Affected Software/OS OpenBSD OpenSSH versions prior to 4.4p1 (unless patched for CVE-2006-5051 and CVE-2008-4109) and 8.5p1 through 9.7p1.
Vulnerability Insight Vendor insights: 1) Race condition in sshd(8) A critical vulnerability in sshd(8) was present that may allow arbitrary code execution with root privileges. Successful exploitation has been demonstrated on 32-bit Linux/glibc systems with ASLR. Under lab conditions, the attack requires on average 6-8 hours of continuous connections up to the maximum the server will accept. Exploitation on 64-bit systems is believed to be possible but has not been demonstrated at this time. It's likely that these attacks will be improved upon. Exploitation on non-glibc systems is conceivable but has not been examined. Systems that lack ASLR or users of downstream Linux distributions that have modified OpenSSH to disable per-connection ASLR re-randomisation (yes - this is a thing, no - we don't understand why) may potentially have an easier path to exploitation. OpenBSD is not vulnerable.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 4.4p1, 8.5p1 - 9.7p1 RCE Vulnerability (regreSSHion) OID:1.3.6.1.4.1.25623.1.0.114680 Version used: 2024-07-09T05:05:54Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.108577)
<div>References</div> <div>cve: CVE-2024-6387</div> <div>url: https://www.openssh.com/txt/release-9.8</div> <div>url: https://www.openssh.com/security.html</div> <div>url: https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt</div> <div>url: https://www.qualys.com/regresshion-cve-2024-6387/</div> <div>url: https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server</div> <div>url: https://unit42.paloaltonetworks.com/threat-brief-cve-2024-6387-openssh/</div> <div>cert-bund: WID-SEC-2024-3195</div> <div>cert-bund: WID-SEC-2024-1725</div> <div>cert-bund: WID-SEC-2024-1486</div> <div>dfn-cert: DFN-CERT-2025-0042</div> <div>dfn-cert: DFN-CERT-2024-1960</div> <div>dfn-cert: DFN-CERT-2024-1959</div> <div>dfn-cert: DFN-CERT-2024-1958</div> <div>dfn-cert: DFN-CERT-2024-1904</div> <div>dfn-cert: DFN-CERT-2024-1869</div> <div>dfn-cert: DFN-CERT-2024-1868</div> <div>dfn-cert: DFN-CERT-2024-1844</div> <div>dfn-cert: DFN-CERT-2024-1759</div> <div>dfn-cert: DFN-CERT-2024-1740</div> <div>dfn-cert: DFN-CERT-2024-1694</div> <div>dfn-cert: DFN-CERT-2024-1693</div>
<div>High (CVSS: 8.1)</div> <div>NVT: OpenBSD OpenSSH < 4.4p1, 8.5p1 - 9.7p1 RCE Vulnerability (regreSSHion)</div>
<div>Product detection result</div> <div>cpe:/a:openbsd:openssh:8.9p1</div> <div>Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)</div>
<div>Summary</div> <div>OpenBSD OpenSSH is prone to a remote code execution (RCE) vulnerability dubbed 'regreSSH-ion'.</div>
<div>Quality of Detection (QoD): 30%</div>
<div>Vulnerability Detection Result</div> <div>Installed version: 8.9p1</div> <div>Fixed version: 9.8</div> <div>Installation</div>
... continues on next page ...

...continued from previous page ...	
path / port:	/usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.8 or later.	
Affected Software/OS OpenBSD OpenSSH versions prior to 4.4p1 (unless patched for CVE-2006-5051 and CVE-2008-4109) and 8.5p1 through 9.7p1.	
Vulnerability Insight Vendor insights: 1) Race condition in sshd(8) A critical vulnerability in sshd(8) was present that may allow arbitrary code execution with root privileges. Successful exploitation has been demonstrated on 32-bit Linux/glibc systems with ASLR. Under lab conditions, the attack requires on average 6-8 hours of continuous connections up to the maximum the server will accept. Exploitation on 64-bit systems is believed to be possible but has not been demonstrated at this time. It's likely that these attacks will be improved upon. Exploitation on non-glibc systems is conceivable but has not been examined. Systems that lack ASLR or users of downstream Linux distributions that have modified OpenSSH to disable per-connection ASLR re-randomisation (yes - this is a thing, no - we don't understand why) may potentially have an easier path to exploitation. OpenBSD is not vulnerable.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 4.4p1, 8.5p1 - 9.7p1 RCE Vulnerability (regreSSHion) OID:1.3.6.1.4.1.25623.1.0.114680 Version used: 2024-07-09T05:05:54Z	
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)	
References cve: CVE-2024-6387 url: https://www.openssh.com/txt/release-9.8 url: https://www.openssh.com/security.html url: https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt url: https://www.qualys.com/regresshion-cve-2024-6387/ url: https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server url: https://unit42.paloaltonetworks.com/threat-brief-cve-2024-6387-openssh/	
... continues on next page ...	

...continued from previous page ...
cert-bund: WID-SEC-2024-3195
cert-bund: WID-SEC-2024-1725
cert-bund: WID-SEC-2024-1486
dfn-cert: DFN-CERT-2025-0042
dfn-cert: DFN-CERT-2024-1960
dfn-cert: DFN-CERT-2024-1959
dfn-cert: DFN-CERT-2024-1958
dfn-cert: DFN-CERT-2024-1904
dfn-cert: DFN-CERT-2024-1869
dfn-cert: DFN-CERT-2024-1868
dfn-cert: DFN-CERT-2024-1844
dfn-cert: DFN-CERT-2024-1759
dfn-cert: DFN-CERT-2024-1740
dfn-cert: DFN-CERT-2024-1694
dfn-cert: DFN-CERT-2024-1693

High (CVSS: 8.1) NVT: OpenBSD OpenSSH < 4.4p1, 8.5p1 - 9.7p1 RCE Vulnerability (regreSSHion)
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to a remote code execution (RCE) vulnerability dubbed 'regreSSH-ion'.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.8 Installation path / port: /usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.8 or later.
Affected Software/OS OpenBSD OpenSSH versions prior to 4.4p1 (unless patched for CVE-2006-5051 and CVE-2008-4109) and 8.5p1 through 9.7p1.
Vulnerability Insight Vendor insights:
... continues on next page ...

...continued from previous page ...
<p>1) Race condition in sshd(8)</p> <p>A critical vulnerability in sshd(8) was present that may allow arbitrary code execution with root privileges.</p> <p>Successful exploitation has been demonstrated on 32-bit Linux/glibc systems with ASLR. Under lab conditions, the attack requires on average 6-8 hours of continuous connections up to the maximum the server will accept. Exploitation on 64-bit systems is believed to be possible but has not been demonstrated at this time. It's likely that these attacks will be improved upon.</p> <p>Exploitation on non-glibc systems is conceivable but has not been examined. Systems that lack ASLR or users of downstream Linux distributions that have modified OpenSSH to disable per-connection ASLR re-randomisation (yes - this is a thing, no - we don't understand why) may potentially have an easier path to exploitation.</p> <p>OpenBSD is not vulnerable.</p>
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: OpenBSD OpenSSH < 4.4p1, 8.5p1 - 9.7p1 RCE Vulnerability (regreSSHion)</p> <p>OID:1.3.6.1.4.1.25623.1.0.114680</p> <p>Version used: 2024-07-09T05:05:54Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:openbsd:openssh:8.9p1</p> <p>Method: OpenSSH Detection Consolidation</p> <p>OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>References</p> <p>cve: CVE-2024-6387</p> <p>url: https://www.openssh.com/txt/release-9.8</p> <p>url: https://www.openssh.com/security.html</p> <p>url: https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt</p> <p>url: https://www.qualys.com/regresshion-cve-2024-6387/</p> <p>url: https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server</p> <p>url: https://unit42.paloaltonetworks.com/threat-brief-cve-2024-6387-openssh/</p> <p>cert-bund: WID-SEC-2024-3195</p> <p>cert-bund: WID-SEC-2024-1725</p> <p>cert-bund: WID-SEC-2024-1486</p> <p>dfn-cert: DFN-CERT-2025-0042</p> <p>dfn-cert: DFN-CERT-2024-1960</p> <p>dfn-cert: DFN-CERT-2024-1959</p> <p>dfn-cert: DFN-CERT-2024-1958</p> <p>dfn-cert: DFN-CERT-2024-1904</p> <p>dfn-cert: DFN-CERT-2024-1869</p> <p>dfn-cert: DFN-CERT-2024-1868</p> <p>dfn-cert: DFN-CERT-2024-1844</p> <p>dfn-cert: DFN-CERT-2024-1759</p> <p>dfn-cert: DFN-CERT-2024-1740</p>
...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2024-1694 dfn-cert: DFN-CERT-2024-1693
High (CVSS: 8.1) NVT: OpenBSD OpenSSH < 4.4p1, 8.5p1 - 9.7p1 RCE Vulnerability (regreSSHion)
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to a remote code execution (RCE) vulnerability dubbed 'regreSSH-ion'.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.8 Installation path / port: /snap/core22/1748/usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.8 or later.
Affected Software/OS OpenBSD OpenSSH versions prior to 4.4p1 (unless patched for CVE-2006-5051 and CVE-2008-4109) and 8.5p1 through 9.7p1.
Vulnerability Insight Vendor insights: 1) Race condition in sshd(8) A critical vulnerability in sshd(8) was present that may allow arbitrary code execution with root privileges. Successful exploitation has been demonstrated on 32-bit Linux/glibc systems with ASLR. Under lab conditions, the attack requires on average 6-8 hours of continuous connections up to the maximum the server will accept. Exploitation on 64-bit systems is believed to be possible but has not been demonstrated at this time. It's likely that these attacks will be improved upon. Exploitation on non-glibc systems is conceivable but has not been examined. Systems that lack ASLR or users of downstream Linux distributions that have modified OpenSSH to disable per-connection ASLR re-randomisation (yes - this is a thing, no - we don't understand why) may potentially have an easier path to exploitation. OpenBSD is not vulnerable.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 4.4p1, 8.5p1 - 9.7p1 RCE Vulnerability (regreSSHion) OID:1.3.6.1.4.1.25623.1.0.114680 Version used: 2024-07-09T05:05:54Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2024-6387 url: https://www.openssh.com/txt/release-9.8 url: https://www.openssh.com/security.html url: https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt url: https://www.qualys.com/regresshion-cve-2024-6387/ url: https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server url: https://unit42.paloaltonetworks.com/threat-brief-cve-2024-6387-openssh/ cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-1725 cert-bund: WID-SEC-2024-1486 dfn-cert: DFN-CERT-2025-0042 dfn-cert: DFN-CERT-2024-1960 dfn-cert: DFN-CERT-2024-1959 dfn-cert: DFN-CERT-2024-1958 dfn-cert: DFN-CERT-2024-1904 dfn-cert: DFN-CERT-2024-1869 dfn-cert: DFN-CERT-2024-1868 dfn-cert: DFN-CERT-2024-1844 dfn-cert: DFN-CERT-2024-1759 dfn-cert: DFN-CERT-2024-1740 dfn-cert: DFN-CERT-2024-1694 dfn-cert: DFN-CERT-2024-1693
High (CVSS: 7.8) NVT: OpenSSL DoS Vulnerability (20240903) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary ... continues on next page ...

...continued from previous page ...
OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.15 Installation path / port: /snap/core22/1612/usr/bin/openssl
Impact Abnormal termination of an application can cause a denial of service.
Solution: Solution type: VendorFix Update to version 3.0.15, 3.1.7, 3.2.3, 3.3.2 or later.
Affected Software/OS OpenSSL versions 3.0, 3.1, 3.2 and 3.3.
Vulnerability Insight Applications performing certificate name checks (e.g., TLS clients checking server certificates) may attempt to read an invalid memory address resulting in abnormal termination of the application process.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20240903) - Linux OID: 1.3.6.1.4.1.25623.1.0.153009 Version used: 2024-09-05T05:05:57Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2024-6119 url: https://openssl-library.org/news/secadv/20240903.txt url: https://openssl-library.org/news/vulnerabilities/index.html cert-bund: WID-SEC-2025-0148 cert-bund: WID-SEC-2025-0001 cert-bund: WID-SEC-2024-3201 cert-bund: WID-SEC-2024-2040 dfn-cert: DFN-CERT-2025-0041
... continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2024-3300
dfn-cert: DFN-CERT-2024-3152
dfn-cert: DFN-CERT-2024-2783
dfn-cert: DFN-CERT-2024-2734
dfn-cert: DFN-CERT-2024-2322
dfn-cert: DFN-CERT-2024-2285

High (CVSS: 7.8) NVT: OpenSSL DoS Vulnerability (20240903) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.15 Installation path / port: /usr/bin/openssl
Impact Abnormal termination of an application can a cause a denial of service.
Solution: Solution type: VendorFix Update to version 3.0.15, 3.1.7, 3.2.3, 3.3.2 or later.
Affected Software/OS OpenSSL versions 3.0, 3.1, 3.2 and 3.3.
Vulnerability Insight Applications performing certificate name checks (e.g., TLS clients checking server certificates) may attempt to read an invalid memory address resulting in abnormal termination of the application process.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20240903) - Linux OID:1.3.6.1.4.1.25623.1.0.153009
... continues on next page ...

...continued from previous page ...
Version used: 2024-09-05T05:05:57Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2024-6119 url: https://openssl-library.org/news/secadv/20240903.txt url: https://openssl-library.org/news/vulnerabilities/index.html cert-bund: WID-SEC-2025-0148 cert-bund: WID-SEC-2025-0001 cert-bund: WID-SEC-2024-3201 cert-bund: WID-SEC-2024-2040 dfn-cert: DFN-CERT-2025-0041 dfn-cert: DFN-CERT-2024-3300 dfn-cert: DFN-CERT-2024-3152 dfn-cert: DFN-CERT-2024-2783 dfn-cert: DFN-CERT-2024-2734 dfn-cert: DFN-CERT-2024-2322 dfn-cert: DFN-CERT-2024-2285

High (CVSS: 7.8) NVT: OpenSSL DoS Vulnerability (20240903) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.15 Installation path / port: /snap/core22/1748/usr/bin/openssl
Impact Abnormal termination of an application can a cause a denial of service.
Solution:
... continues on next page ...

...continued from previous page ...
Solution type: VendorFix Update to version 3.0.15, 3.1.7, 3.2.3, 3.3.2 or later.
Affected Software/OS OpenSSL versions 3.0, 3.1, 3.2 and 3.3.
Vulnerability Insight Applications performing certificate name checks (e.g., TLS clients checking server certificates) may attempt to read an invalid memory address resulting in abnormal termination of the application process.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20240903) - Linux OID:1.3.6.1.4.1.25623.1.0.153009 Version used: 2024-09-05T05:05:57Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2024-6119 url: https://openssl-library.org/news/secadv/20240903.txt url: https://openssl-library.org/news/vulnerabilities/index.html cert-bund: WID-SEC-2025-0148 cert-bund: WID-SEC-2025-0001 cert-bund: WID-SEC-2024-3201 cert-bund: WID-SEC-2024-2040 dfn-cert: DFN-CERT-2025-0041 dfn-cert: DFN-CERT-2024-3300 dfn-cert: DFN-CERT-2024-3152 dfn-cert: DFN-CERT-2024-2783 dfn-cert: DFN-CERT-2024-2734 dfn-cert: DFN-CERT-2024-2322 dfn-cert: DFN-CERT-2024-2285
High (CVSS: 7.8) NVT: PHP < 8.0.27, 8.1.x < 8.1.14, 8.2.x < 8.2.1 Security Update - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
... continues on next page ...

...continued from previous page ...
Summary PHP is prone to an integer overflow vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 8.0.27 Installation path / port: /usr/bin/php7.2
Solution: Solution type: VendorFix Update to version 8.0.27, 8.1.14, 8.2.1 or later.
Affected Software/OS PHP prior to version 8.0.27, version 8.1.x through 8.1.13 and 8.2.0.
Vulnerability Insight Due to an uncaught integer overflow, PDO::quote() of PDO_SQLite may return a not properly quoted string.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 8.0.27, 8.1.x < 8.1.14, 8.2.x < 8.2.1 Security Update - Linux OID:1.3.6.1.4.1.25623.1.0.149069 Version used: 2023-01-09T10:12:48Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2022-31631 url: https://www.php.net/ChangeLog-8.php#8.0.27 url: https://www.php.net/ChangeLog-8.php#8.1.14 url: https://www.php.net/ChangeLog-8.php#8.2.1 cert-bund: WID-SEC-2023-0035 dfn-cert: DFN-CERT-2023-0435 dfn-cert: DFN-CERT-2023-0422 dfn-cert: DFN-CERT-2023-0071 dfn-cert: DFN-CERT-2023-0034

<div>High (CVSS: 7.8) NVT: LibreOffice Improper Digital Signature Invalidation Vulnerability (Sep 2024) - Linux</div>
<div>Product detection result cpe:/a:libreoffice:libreoffice:7.3.7.2.2 Detected by LibreOffice Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.25623 ↪.1.0.902701)</div>
<div>Summary LibreOffice is prone to an improper digital signature invalidation vulnerability.</div>
<div>Quality of Detection (QoD): 30%</div>
<div>Vulnerability Detection Result Installed version: 7.3.7.2.2 Fixed version: 24.2.5 or 24.8.0 Installation path / port: /usr/bin/libreoffice</div>
<div>Impact Successful exploitation allows an attacker to exploit the repair mechanism to bypass signature verification.</div>
<div>Solution: Solution type: VendorFix Update to version 24.2.5 or 24.8.0 or later.</div>
<div>Affected Software/OS LibreOffice version before 24.2.5 on Linux.</div>
<div>Vulnerability Insight The flaw exists due to an incorrect digital signature validation during the repair of corrupt zip files in LibreOffice.</div>
<div>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: LibreOffice Improper Digital Signature Invalidation Vulnerability (Sep 2024) - . ↪.. OID:1.3.6.1.4.1.25623.1.0.834622 Version used: 2024-10-18T15:39:59Z</div>
<div>Product Detection Result Product: cpe:/a:libreoffice:libreoffice:7.3.7.2.2 Method: LibreOffice Detection (Linux/Unix SSH Login) OID: 1.3.6.1.4.1.25623.1.0.902701</div>
<div>... continues on next page ...</div>

...continued from previous page ...
<div>References</div> <div>cve: CVE-2024-7788</div> <div>url: https://www.libreoffice.org/about-us/security/advisories/CVE-2024-7788</div> <div>url: https://access.redhat.com/security/cve/cve-2024-7788</div> <div>cert-bund: WID-SEC-2024-2171</div> <div>dfn-cert: DFN-CERT-2024-2464</div>
<div>High (CVSS: 7.8)</div> <div>NVT: Mozilla Firefox Security Advisory (MFSA2024-53) - Linux</div>
<div>Product detection result</div> <div>cpe:/a:mozilla:firefox:136.0</div> <div>Detected by Mozilla Firefox Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.2↪5623.1.0.800017)</div>
<div>Summary</div> <div>This host is missing a security update for Mozilla Firefox.</div>
<div>Quality of Detection (QoD): 30%</div>
<div>Vulnerability Detection Result</div> <div>Installed version: 130.0</div> <div>Fixed version: 131.0.3</div> <div>Installation</div> <div>path / port: /snap/firefox/4848/usr/lib/firefox/firefox</div>
<div>Solution:</div> <div>Solution type: VendorFix</div> <div>The vendor has released an update. Please see the reference(s) for more information.</div>
<div>Affected Software/OS</div> <div>Firefox version(s) below 131.0.3.</div>
<div>Vulnerability Insight</div> <div>CVE-2024-9936: Undefined behavior in selection node cache When manipulating the selection node cache, an attacker may have been able to cause unexpected behavior, potentially leading to an exploitable crash.</div>
<div>Vulnerability Detection Method</div> <div>Checks if a vulnerable package version is present on the target host.</div> <div>Details: Mozilla Firefox Security Advisory (MFSA2024-53) - Linux</div> <div>OID:1.3.6.1.4.1.25623.1.2.1.2024.53</div> <div>Version used: 2024-10-15T05:05:49Z</div>
... continues on next page ...

...continued from previous page...

Product Detection Result

Product: cpe:/a:mozilla:firefox:136.0

Method: Mozilla Firefox Detection (Linux/Unix SSH Login)

OID: 1.3.6.1.4.1.25623.1.0.800017)

References

cve: CVE-2024-9936

advisory-id: MFSa2024-53

url: <https://www.mozilla.org/en-US/security/advisories/mfsa2024-53/>url: https://bugzilla.mozilla.org/show_bug.cgi?id=1920381

cert-bund: WID-SEC-2024-3174

dfn-cert: DFN-CERT-2024-2705

High (CVSS: 7.8)

NVT: Intel BIOS Privilege Escalation Vulnerability (INTEL-SA-00686)

Summary

The Intel BIOS on the remote host might be prone to a privilege escalation vulnerability.

Quality of Detection (QoD): 1%**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

Solution:**Solution type:** Mitigation

Intel is releasing BIOS updates to mitigate this potential vulnerability.

Vulnerability Insight

Out-of-bounds write in the BIOS firmware for some Intel(R) Processors may allow an authenticated user to potentially enable escalation of privilege via local access.

Vulnerability Detection Method

Checks if the remote host is using an Intel CPU.

Details: Intel BIOS Privilege Escalation Vulnerability (INTEL-SA-00686)

OID:1.3.6.1.4.1.25623.1.0.104316

Version used: 2023-10-18T05:05:17Z

References

cve: CVE-2021-33060

url: <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00686.html>

cert-bund: WID-SEC-2022-0994

dfn-cert: DFN-CERT-2022-1774

High (CVSS: 7.5) NVT: Samba Multiple Vulnerabilities (Sep 2022)
Product detection result cpe:/a:samba:samba:4.15.13 Detected by Samba Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800403)
Summary Samba is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 4.15.13 Fixed version: 4.17.0 Installation path / port: /usr/sbin/smbd
Solution: Solution type: VendorFix Update to version 4.17.0 or later.
Affected Software/OS Samba versions starting from 4.1 and prior to 4.17.0.
Vulnerability Insight The following flaws exist: - CVE-2022-1615: In Samba, GnuTLS gnutls_rnd() can fail and give predictable random values. - CVE-2022-32743: Samba does not validate the Validated-DNS-Host-Name right for the dNSHostName attribute which could permit unprivileged users to write it.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Samba Multiple Vulnerabilities (Sep 2022) OID:1.3.6.1.4.1.25623.1.0.104323 Version used: 2023-10-19T05:05:21Z
Product Detection Result Product: cpe:/a:samba:samba:4.15.13 Method: Samba Version Detection OID: 1.3.6.1.4.1.25623.1.0.800403)
References cve: CVE-2022-1615 cve: CVE-2022-32743 ... continues on next page ...

...continued from previous page ...
url: https://bugzilla.samba.org/show_bug.cgi?id=15103
url: https://gitlab.com/samba-team/samba/-/merge_requests/2644
url: https://bugzilla.samba.org/show_bug.cgi?id=14833
cert-bund: WID-SEC-2022-1229
cert-bund: WID-SEC-2022-1179
dfn-cert: DFN-CERT-2024-0231
dfn-cert: DFN-CERT-2023-2792
dfn-cert: DFN-CERT-2022-2000

High (CVSS: 7.5)

NVT: OpenSSL: Using a Custom Cipher with NID_undef may lead to NULL encryption (CVE-2022-3358) - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 3.0.2

Fixed version: 3.0.6

Installation

path / port: /usr/bin/openssl

Solution:

Solution type: VendorFix

Update to version 3.0.6 or later.

Affected Software/OS

OpenSSL versions 3.0.0 through 3.0.5.

Vulnerability Insight

OpenSSL supports creating a custom cipher via the legacy `EVP_CIPHER_meth_new()` function and associated function calls. This function was deprecated in OpenSSL 3.0 and application authors are instead encouraged to use the new provider mechanism in order to implement custom ciphers.

... continues on next page ...

...continued from previous page...	
<p>OpenSSL versions 3.0.0 to 3.0.5 incorrectly handle legacy custom ciphers passed to the <code>EVP_EncryptInit_ex2()</code>, <code>EVP_DecryptInit_ex2()</code> and <code>EVP_CipherInit_ex2()</code> functions (as well as other similarly named encryption and decryption initialisation functions). Instead of using the custom cipher directly it incorrectly tries to fetch an equivalent cipher from the available providers. An equivalent cipher is found based on the NID passed to <code>EVP_CIPHER_meth_new()</code>. This NID is supposed to represent the unique NID for a given cipher. However it is possible for an application to incorrectly pass <code>NID_undef</code> as this value in the call to <code>EVP_CIPHER_meth_new()</code>. When <code>NID_undef</code> is used in this way the OpenSSL encryption/decryption initialisation function will match the NULL cipher as being equivalent and will fetch this from the available providers. This will succeed if the default provider has been loaded (or if a third party provider has been loaded that offers this cipher). Using the NULL cipher means that the plaintext is emitted as the ciphertext.</p> <p>Applications are only affected by this issue if they call <code>EVP_CIPHER_meth_new()</code> using <code>NID_undef</code> and subsequently use it in a call to an encryption/decryption initialisation function. Applications that only use SSL/TLS are not impacted by this issue.</p>	
Vulnerability Detection Method	
<p>Checks if a vulnerable version is present on the target host.</p> <p>Details: OpenSSL: Using a Custom Cipher with NID_undef may lead to NULL encryption (CVE-.. ↪..</p> <p>OID:1.3.6.1.4.1.25623.1.0.104353</p> <p>Version used: 2023-10-19T05:05:21Z</p>	
Product Detection Result	
<p>Product: <code>cpe:/a:openssl:openssl:3.0.2</code></p> <p>Method: OpenSSL Detection Consolidation</p> <p>OID: 1.3.6.1.4.1.25623.1.0.145462)</p>	
References	
<p>cve: CVE-2022-3358</p> <p>url: https://www.openssl.org/news/secadv/20221011.txt</p> <p>cert-bund: WID-SEC-2023-1542</p> <p>cert-bund: WID-SEC-2022-1690</p> <p>dfn-cert: DFN-CERT-2023-0329</p> <p>dfn-cert: DFN-CERT-2022-2444</p> <p>dfn-cert: DFN-CERT-2022-2244</p>	
<p>High (CVSS: 7.5)</p> <p>NVT: OpenSSL: X.509 Policy Constraints Double Locking Vulnerability (Dec 2022) - Linux</p>	
Product detection result	
<p><code>cpe:/a:openssl:openssl:3.0.2</code></p> <p>Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)</p>	
Summary	
... continues on next page ...	

...continued from previous page ...
OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.8 Installation path / port: /usr/bin/openssl
Solution: Solution type: VendorFix Update to version 3.0.8 or later.
Affected Software/OS OpenSSL versions 3.0.0 through 3.0.7.
Vulnerability Insight If an X.509 certificate contains a malformed policy constraint and policy processing is enabled, then a write lock will be taken twice recursively. On some operating systems (most widely: Windows) this results in a denial of service when the affected process hangs. Policy processing being enabled on a publicly facing server is not considered to be a common setup. Policy processing is enabled by passing the '-policy' argument to the command line utilities or by calling either 'X509_VERIFY_PARAM_add0_policy()' or 'X509_VERIFY_PARAM_set1_policies()' functions.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL: X.509 Policy Constraints Double Locking Vulnerability (Dec 2022) - Lin. ↔.. OID:1.3.6.1.4.1.25623.1.0.149016 Version used: 2023-10-19T05:05:21Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2022-3996 url: https://www.openssl.org/news/secadv/20221213.txt cert-bund: WID-SEC-2022-2310 dfn-cert: DFN-CERT-2023-0960 dfn-cert: DFN-CERT-2023-0661 dfn-cert: DFN-CERT-2023-0639
... continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2022-2898
 dfn-cert: DFN-CERT-2022-2831

High (CVSS: 7.5)**NVT: OpenSSL 3.0 < 3.0.8 Multiple Vulnerabilities - Linux****Product detection result**

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 3.0.2

Fixed version: 3.0.8

Installation

path / port: /snap/core22/1612/usr/bin/openssl

Solution:**Solution type:** VendorFix

Update to version 3.0.8 or later.

Affected Software/OS

OpenSSL version 3.0.

Vulnerability Insight

The following flaws exist:

- CVE-2022-4203: X.509 Name Constraints Read Buffer Overflow
- CVE-2023-0216: Invalid pointer dereference in d2i_PKCS7 functions
- CVE-2023-0217: NULL dereference validating DSA public key
- CVE-2023-0401: NULL dereference during PKCS7 data verification

Vulnerability Detection Method

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

Details: OpenSSL 3.0 < 3.0.8 Multiple Vulnerabilities - Linux

OID:1.3.6.1.4.1.25623.1.0.104533

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

Product Detection Result

Product: cpe:/a:openssl:openssl:3.0.2

Method: OpenSSL Detection Consolidation

... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2022-4203 cve: CVE-2023-0216 cve: CVE-2023-0217 cve: CVE-2023-0401 url: https://www.openssl.org/news/secadv/20230207.txt cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-0304 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-0016 dfn-cert: DFN-CERT-2023-1162 dfn-cert: DFN-CERT-2023-0884 dfn-cert: DFN-CERT-2023-0661 dfn-cert: DFN-CERT-2023-0639 dfn-cert: DFN-CERT-2023-0618 dfn-cert: DFN-CERT-2023-0329 dfn-cert: DFN-CERT-2023-0284

High (CVSS: 7.5) NVT: OpenSSL 1.0.2 < 1.0.2zg, 1.1.1 < 1.1.1t, 3.0 < 3.0.8 Multiple Vulnerabilities - Linux
Product detection result cpe: /a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.8 Installation path / port: /usr/bin/openssl
Solution: Solution type: VendorFix Update to version 1.0.2zg, 1.1.1t, 3.0.8 or later.
Affected Software/OS
... continues on next page ...

...continued from previous page ...
OpenSSL version 1.0.2, 1.1.1 and 3.0.
Vulnerability Insight The following flaws exist: - CVE-2022-4304: Timing Oracle in RSA Decryption - CVE-2023-0215: Use-after-free following BIO_new_NDEF - CVE-2023-0286: X.400 address type confusion in X.509 GeneralName
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL 1.0.2 < 1.0.2zg, 1.1.1 < 1.1.1t, 3.0 < 3.0.8 Multiple Vulnerabilities -. ↔.. OID:1.3.6.1.4.1.25623.1.0.104531 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2022-4304 cve: CVE-2023-0215 cve: CVE-2023-0286 url: https://www.openssl.org/news/secadv/20230207.txt cert-bund: WID-SEC-2024-2086 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2023-2031 cert-bund: WID-SEC-2023-1886 cert-bund: WID-SEC-2023-1812 cert-bund: WID-SEC-2023-1793 cert-bund: WID-SEC-2023-1790 cert-bund: WID-SEC-2023-1553 cert-bund: WID-SEC-2023-1432 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-1350 cert-bund: WID-SEC-2023-1033 cert-bund: WID-SEC-2023-0304 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-0147 dfn-cert: DFN-CERT-2024-0016 dfn-cert: DFN-CERT-2023-2192 dfn-cert: DFN-CERT-2023-1760 dfn-cert: DFN-CERT-2023-1697
... continues on next page ...

...continued from previous page ...	
dfn-cert:	DFN-CERT-2023-1656
dfn-cert:	DFN-CERT-2023-1590
dfn-cert:	DFN-CERT-2023-1462
dfn-cert:	DFN-CERT-2023-1423
dfn-cert:	DFN-CERT-2023-1297
dfn-cert:	DFN-CERT-2023-1256
dfn-cert:	DFN-CERT-2023-1162
dfn-cert:	DFN-CERT-2023-1043
dfn-cert:	DFN-CERT-2023-0885
dfn-cert:	DFN-CERT-2023-0884
dfn-cert:	DFN-CERT-2023-0774
dfn-cert:	DFN-CERT-2023-0662
dfn-cert:	DFN-CERT-2023-0661
dfn-cert:	DFN-CERT-2023-0639
dfn-cert:	DFN-CERT-2023-0543
dfn-cert:	DFN-CERT-2023-0471
dfn-cert:	DFN-CERT-2023-0430
dfn-cert:	DFN-CERT-2023-0329
dfn-cert:	DFN-CERT-2023-0318
dfn-cert:	DFN-CERT-2023-0310
dfn-cert:	DFN-CERT-2023-0299
dfn-cert:	DFN-CERT-2023-0288
dfn-cert:	DFN-CERT-2023-0284
dfn-cert:	DFN-CERT-2023-0283

High (CVSS: 7.5)

NVT: OpenSSL 1.0.2 < 1.0.2zg, 1.1.1 < 1.1.1t, 3.0 < 3.0.8 Multiple Vulnerabilities - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 3.0.2

Fixed version: 3.0.8

Installation

path / port: /snap/core22/1748/usr/bin/openssl

Solution:

Solution type: VendorFix

Update to version 1.0.2zg, 1.1.1t, 3.0.8 or later.

... continues on next page ...

...continued from previous page ...
Affected Software/OS OpenSSL version 1.0.2, 1.1.1 and 3.0.
Vulnerability Insight The following flaws exist: - CVE-2022-4304: Timing Oracle in RSA Decryption - CVE-2023-0215: Use-after-free following BIO_new_NDEF - CVE-2023-0286: X.400 address type confusion in X.509 GeneralName
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL 1.0.2 < 1.0.2zg, 1.1.1 < 1.1.1t, 3.0 < 3.0.8 Multiple Vulnerabilities -. ↪.. OID:1.3.6.1.4.1.25623.1.0.104531 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2022-4304 cve: CVE-2023-0215 cve: CVE-2023-0286 url: https://www.openssl.org/news/secadv/20230207.txt cert-bund: WID-SEC-2024-2086 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2023-2031 cert-bund: WID-SEC-2023-1886 cert-bund: WID-SEC-2023-1812 cert-bund: WID-SEC-2023-1793 cert-bund: WID-SEC-2023-1790 cert-bund: WID-SEC-2023-1553 cert-bund: WID-SEC-2023-1432 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-1350 cert-bund: WID-SEC-2023-1033 cert-bund: WID-SEC-2023-0304 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-0147 dfn-cert: DFN-CERT-2024-0016
...continues on next page ...

...continued from previous page ...

```

dfn-cert: DFN-CERT-2023-2192
dfn-cert: DFN-CERT-2023-1760
dfn-cert: DFN-CERT-2023-1697
dfn-cert: DFN-CERT-2023-1656
dfn-cert: DFN-CERT-2023-1590
dfn-cert: DFN-CERT-2023-1462
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1297
dfn-cert: DFN-CERT-2023-1256
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-1043
dfn-cert: DFN-CERT-2023-0885
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0774
dfn-cert: DFN-CERT-2023-0662
dfn-cert: DFN-CERT-2023-0661
dfn-cert: DFN-CERT-2023-0639
dfn-cert: DFN-CERT-2023-0543
dfn-cert: DFN-CERT-2023-0471
dfn-cert: DFN-CERT-2023-0430
dfn-cert: DFN-CERT-2023-0329
dfn-cert: DFN-CERT-2023-0318
dfn-cert: DFN-CERT-2023-0310
dfn-cert: DFN-CERT-2023-0299
dfn-cert: DFN-CERT-2023-0288
dfn-cert: DFN-CERT-2023-0284
dfn-cert: DFN-CERT-2023-0283

```

High (CVSS: 7.5)

NVT: OpenSSL 1.0.2 < 1.0.2zg, 1.1.1 < 1.1.1t, 3.0 < 3.0.8 Multiple Vulnerabilities - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 3.0.2

Fixed version: 3.0.8

Installation

path / port: /snap/core22/1612/usr/bin/openssl

... continues on next page ...

...continued from previous page ...
Solution: Solution type: VendorFix Update to version 1.0.2zg, 1.1.1t, 3.0.8 or later.
Affected Software/OS OpenSSL version 1.0.2, 1.1.1 and 3.0.
Vulnerability Insight The following flaws exist: - CVE-2022-4304: Timing Oracle in RSA Decryption - CVE-2023-0215: Use-after-free following BIO_new_NDEF - CVE-2023-0286: X.400 address type confusion in X.509 GeneralName
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL 1.0.2 < 1.0.2zg, 1.1.1 < 1.1.1t, 3.0 < 3.0.8 Multiple Vulnerabilities -. ↔.. OID:1.3.6.1.4.1.25623.1.0.104531 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2022-4304 cve: CVE-2023-0215 cve: CVE-2023-0286 url: https://www.openssl.org/news/secadv/20230207.txt cert-bund: WID-SEC-2024-2086 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2023-2031 cert-bund: WID-SEC-2023-1886 cert-bund: WID-SEC-2023-1812 cert-bund: WID-SEC-2023-1793 cert-bund: WID-SEC-2023-1790 cert-bund: WID-SEC-2023-1553 cert-bund: WID-SEC-2023-1432 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-1350 cert-bund: WID-SEC-2023-1033
...continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2023-0304 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-0147 dfn-cert: DFN-CERT-2024-0016 dfn-cert: DFN-CERT-2023-2192 dfn-cert: DFN-CERT-2023-1760 dfn-cert: DFN-CERT-2023-1697 dfn-cert: DFN-CERT-2023-1656 dfn-cert: DFN-CERT-2023-1590 dfn-cert: DFN-CERT-2023-1462 dfn-cert: DFN-CERT-2023-1423 dfn-cert: DFN-CERT-2023-1297 dfn-cert: DFN-CERT-2023-1256 dfn-cert: DFN-CERT-2023-1162 dfn-cert: DFN-CERT-2023-1043 dfn-cert: DFN-CERT-2023-0885 dfn-cert: DFN-CERT-2023-0884 dfn-cert: DFN-CERT-2023-0774 dfn-cert: DFN-CERT-2023-0662 dfn-cert: DFN-CERT-2023-0661 dfn-cert: DFN-CERT-2023-0639 dfn-cert: DFN-CERT-2023-0543 dfn-cert: DFN-CERT-2023-0471 dfn-cert: DFN-CERT-2023-0430 dfn-cert: DFN-CERT-2023-0329 dfn-cert: DFN-CERT-2023-0318 dfn-cert: DFN-CERT-2023-0310 dfn-cert: DFN-CERT-2023-0299 dfn-cert: DFN-CERT-2023-0288 dfn-cert: DFN-CERT-2023-0284 dfn-cert: DFN-CERT-2023-0283

High (CVSS: 7.5)

NVT: OpenSSL 3.0 < 3.0.8 Multiple Vulnerabilities - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 3.0.2

...continues on next page ...

...continued from previous page...	
Fixed version:	3.0.8
Installation path / port:	/usr/bin/openssl
Solution: Solution type: VendorFix Update to version 3.0.8 or later.	
Affected Software/OS OpenSSL version 3.0.	
Vulnerability Insight The following flaws exist: - CVE-2022-4203: X.509 Name Constraints Read Buffer Overflow - CVE-2023-0216: Invalid pointer dereference in d2i_PKCS7 functions - CVE-2023-0217: NULL dereference validating DSA public key - CVE-2023-0401: NULL dereference during PKCS7 data verification	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL 3.0 < 3.0.8 Multiple Vulnerabilities - Linux OID:1.3.6.1.4.1.25623.1.0.104533 Version used: 2023-10-13T05:06:10Z	
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)	
References cve: CVE-2022-4203 cve: CVE-2023-0216 cve: CVE-2023-0217 cve: CVE-2023-0401 url: https://www.openssl.org/news/secadv/20230207.txt cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-0304 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-0016 dfn-cert: DFN-CERT-2023-1162 dfn-cert: DFN-CERT-2023-0884 dfn-cert: DFN-CERT-2023-0661 dfn-cert: DFN-CERT-2023-0639 dfn-cert: DFN-CERT-2023-0618	
...continues on next page...	

...continued from previous page ...

dfn-cert: DFN-CERT-2023-0329
dfn-cert: DFN-CERT-2023-0284

High (CVSS: 7.5)**NVT: OpenSSL 3.0 < 3.0.8 Multiple Vulnerabilities - Linux****Product detection result**

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 3.0.2

Fixed version: 3.0.8

Installation

path / port: /snap/core22/1748/usr/bin/openssl

Solution:**Solution type:** VendorFix

Update to version 3.0.8 or later.

Affected Software/OS

OpenSSL version 3.0.

Vulnerability Insight

The following flaws exist:

- CVE-2022-4203: X.509 Name Constraints Read Buffer Overflow
- CVE-2023-0216: Invalid pointer dereference in d2i_PKCS7 functions
- CVE-2023-0217: NULL dereference validating DSA public key
- CVE-2023-0401: NULL dereference during PKCS7 data verification

Vulnerability Detection Method

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

Details: OpenSSL 3.0 < 3.0.8 Multiple Vulnerabilities - Linux

OID:1.3.6.1.4.1.25623.1.0.104533

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

Product Detection Result

Product: cpe:/a:openssl:openssl:3.0.2

Method: OpenSSL Detection Consolidation

... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2022-4203 cve: CVE-2023-0216 cve: CVE-2023-0217 cve: CVE-2023-0401 url: https://www.openssl.org/news/secadv/20230207.txt cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-0304 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-0016 dfn-cert: DFN-CERT-2023-1162 dfn-cert: DFN-CERT-2023-0884 dfn-cert: DFN-CERT-2023-0661 dfn-cert: DFN-CERT-2023-0639 dfn-cert: DFN-CERT-2023-0618 dfn-cert: DFN-CERT-2023-0329 dfn-cert: DFN-CERT-2023-0284

High (CVSS: 7.5)
NVT: Samba Multiple Vulnerabilities (Jul 2023)

Product detection result

cpe:/a:samba:samba:4.15.13

Detected by Samba Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800403)

Summary

Samba is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 4.15.13

Fixed version: 4.16.11 / 4.17.10 / 4.18.5

Installation

path / port: /usr/sbin/smbd

Solution:

Solution type: VendorFix

Update to version 4.16.11, 4.17.10, 4.18.5 or later.

Affected Software/OS

... continues on next page ...

...continued from previous page ...
All versions of Samba up to 4.16.10, 4.17.9 and 4.18.4.
Vulnerability Insight The following flaws exist: - CVE-2022-2127: Out-Of-Bounds read in winbind AUTH_CRAP - CVE-2023-34966: Samba Spotlight mdssvc RPC Request Infinite Loop Denial-of-Service Vulnerability - CVE-2023-34967: Samba Spotlight mdssvc RPC Request Type Confusion Denial-of-Service Vulnerability - CVE-2023-34968: Spotlight server-side Share Path Disclosure
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Samba Multiple Vulnerabilities (Jul 2023) OID:1.3.6.1.4.1.25623.1.0.104872 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:samba:samba:4.15.13 Method: Samba Version Detection OID: 1.3.6.1.4.1.25623.1.0.800403)
References cve: CVE-2022-2127 cve: CVE-2023-34966 cve: CVE-2023-34967 cve: CVE-2023-34968 url: https://www.samba.org/samba/security/CVE-2022-2127.html url: https://www.samba.org/samba/security/CVE-2023-34966.html url: https://www.samba.org/samba/security/CVE-2023-34967.html url: https://www.samba.org/samba/security/CVE-2023-34968.html cert-bund: WID-SEC-2023-2910 cert-bund: WID-SEC-2023-1842 dfn-cert: DFN-CERT-2024-1661 dfn-cert: DFN-CERT-2024-1065 dfn-cert: DFN-CERT-2024-0839 dfn-cert: DFN-CERT-2024-0519 dfn-cert: DFN-CERT-2024-0231 dfn-cert: DFN-CERT-2023-2818 dfn-cert: DFN-CERT-2023-1744 dfn-cert: DFN-CERT-2023-1741 dfn-cert: DFN-CERT-2023-1666

High (CVSS: 7.5) NVT: Samba Missing ACL Vulnerability (CVE-2020-25720)
Product detection result cpe:/a:samba:samba:4.15.13 Detected by Samba Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800403)
Summary Samba is prone to a missing access control list (ACL) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 4.15.13 Fixed version: 4.17.7 Installation path / port: /usr/sbin/smbd
Solution: Solution type: VendorFix Update to version 4.17.7 or later.
Affected Software/OS Samba version starting from 4.1 and prior to 4.17.7.
Vulnerability Insight A vulnerability was found in Samba where a delegated administrator with permission to create objects in Active Directory can write to all attributes of the newly created object, including security-sensitive attributes, even after the object's creation. This issue occurs because the administrator owns the object due to the lack of an Access Control List (ACL) at the time of creation and later being recognized as the 'creator owner.' The retained significant rights of the delegated administrator may not be well understood, potentially leading to unintended privilege escalation or security risks.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Samba Missing ACL Vulnerability (CVE-2020-25720) OID:1.3.6.1.4.1.25623.1.0.114865 Version used: 2024-11-26T07:35:52Z
Product Detection Result Product: cpe:/a:samba:samba:4.15.13 Method: Samba Version Detection OID: 1.3.6.1.4.1.25623.1.0.800403)
... continues on next page ...

...continued from previous page ...
References cve: CVE-2020-25720 url: https://www.samba.org/samba/history/samba-4.17.7.html url: https://bugzilla.samba.org/show_bug.cgi?id=14810 url: https://gitlab.com/samba-team/samba/-/merge_requests/2514 dfn-cert: DFN-CERT-2024-0519
High (CVSS: 7.5) NVT: OpenSSL: Using a Custom Cipher with NID_undef may lead to NULL encryption (CVE-2022-3358) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.6 Installation path / port: /snap/core22/1748/usr/bin/openssl
Solution: Solution type: VendorFix Update to version 3.0.6 or later.
Affected Software/OS OpenSSL versions 3.0.0 through 3.0.5.
Vulnerability Insight OpenSSL supports creating a custom cipher via the legacy EVP_CIPHER_meth_new() function and associated function calls. This function was deprecated in OpenSSL 3.0 and application authors are instead encouraged to use the new provider mechanism in order to implement custom ciphers.
... continues on next page ...

...continued from previous page ...	
<p>OpenSSL versions 3.0.0 to 3.0.5 incorrectly handle legacy custom ciphers passed to the <code>EVP_EncryptInit_ex2()</code>, <code>EVP_DecryptInit_ex2()</code> and <code>EVP_CipherInit_ex2()</code> functions (as well as other similarly named encryption and decryption initialisation functions). Instead of using the custom cipher directly it incorrectly tries to fetch an equivalent cipher from the available providers. An equivalent cipher is found based on the NID passed to <code>EVP_CIPHER_meth_new()</code>. This NID is supposed to represent the unique NID for a given cipher. However it is possible for an application to incorrectly pass <code>NID_undef</code> as this value in the call to <code>EVP_CIPHER_meth_new()</code>. When <code>NID_undef</code> is used in this way the OpenSSL encryption/decryption initialisation function will match the NULL cipher as being equivalent and will fetch this from the available providers. This will succeed if the default provider has been loaded (or if a third party provider has been loaded that offers this cipher). Using the NULL cipher means that the plaintext is emitted as the ciphertext.</p> <p>Applications are only affected by this issue if they call <code>EVP_CIPHER_meth_new()</code> using <code>NID_undef</code> and subsequently use it in a call to an encryption/decryption initialisation function. Applications that only use SSL/TLS are not impacted by this issue.</p>	
Vulnerability Detection Method	
<p>Checks if a vulnerable version is present on the target host.</p> <p>Details: OpenSSL: Using a Custom Cipher with <code>NID_undef</code> may lead to NULL encryption (CVE- ↪...</p> <p>OID: 1.3.6.1.4.1.25623.1.0.104353</p> <p>Version used: 2023-10-19T05:05:21Z</p>	
Product Detection Result	
<p>Product: <code>cpe:/a:openssl:openssl:3.0.2</code></p> <p>Method: OpenSSL Detection Consolidation</p> <p>OID: 1.3.6.1.4.1.25623.1.0.145462)</p>	
References	
<p>cve: CVE-2022-3358</p> <p>url: https://www.openssl.org/news/secadv/20221011.txt</p> <p>cert-bund: WID-SEC-2023-1542</p> <p>cert-bund: WID-SEC-2022-1690</p> <p>dfn-cert: DFN-CERT-2023-0329</p> <p>dfn-cert: DFN-CERT-2022-2444</p> <p>dfn-cert: DFN-CERT-2022-2244</p>	
<p>High (CVSS: 7.5)</p> <p>NVT: OpenSSL: Using a Custom Cipher with <code>NID_undef</code> may lead to NULL encryption (CVE-2022-3358) - Linux</p>	
Product detection result	
<p><code>cpe:/a:openssl:openssl:3.0.2</code></p> <p>Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)</p>	
... continues on next page ...	

...continued from previous page ...	
Summary	OpenSSL is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 30%	
Vulnerability Detection Result	Installed version: 3.0.2 Fixed version: 3.0.6 Installation path / port: /snap/core22/1612/usr/bin/openssl
Solution:	Solution type: VendorFix Update to version 3.0.6 or later.
Affected Software/OS	OpenSSL versions 3.0.0 through 3.0.5.
Vulnerability Insight	<p>OpenSSL supports creating a custom cipher via the legacy <code>EVP_CIPHER_meth_new()</code> function and associated function calls. This function was deprecated in OpenSSL 3.0 and application authors are instead encouraged to use the new provider mechanism in order to implement custom ciphers.</p> <p>OpenSSL versions 3.0.0 to 3.0.5 incorrectly handle legacy custom ciphers passed to the <code>EVP_EncryptInit_ex2()</code>, <code>EVP_DecryptInit_ex2()</code> and <code>EVP_CipherInit_ex2()</code> functions (as well as other similarly named encryption and decryption initialisation functions). Instead of using the custom cipher directly it incorrectly tries to fetch an equivalent cipher from the available providers. An equivalent cipher is found based on the NID passed to <code>EVP_CIPHER_meth_new()</code>. This NID is supposed to represent the unique NID for a given cipher. However it is possible for an application to incorrectly pass <code>NID_undef</code> as this value in the call to <code>EVP_CIPHER_meth_new()</code>. When <code>NID_undef</code> is used in this way the OpenSSL encryption/decryption initialisation function will match the NULL cipher as being equivalent and will fetch this from the available providers. This will succeed if the default provider has been loaded (or if a third party provider has been loaded that offers this cipher). Using the NULL cipher means that the plaintext is emitted as the ciphertext.</p> <p>Applications are only affected by this issue if they call <code>EVP_CIPHER_meth_new()</code> using <code>NID_undef</code> and subsequently use it in a call to an encryption/decryption initialisation function. Applications that only use SSL/TLS are not impacted by this issue.</p>
Vulnerability Detection Method	Checks if a vulnerable version is present on the target host. Details: OpenSSL: Using a Custom Cipher with NID_undef may lead to NULL encryption (CVE- ↪... OID:1.3.6.1.4.1.25623.1.0.104353 Version used: 2023-10-19T05:05:21Z
... continues on next page ...	

...continued from previous page ...
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2022-3358 url: https://www.openssl.org/news/secadv/20221011.txt cert-bund: WID-SEC-2023-1542 cert-bund: WID-SEC-2022-1690 dfn-cert: DFN-CERT-2023-0329 dfn-cert: DFN-CERT-2022-2444 dfn-cert: DFN-CERT-2022-2244

High (CVSS: 7.5) NVT: Apache HTTP Server < 2.4.58 'mod_macro' Out-of-bounds Read Vulnerability - Linux
Product detection result cpe:/a:apache:http_server:2.4.52 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1 ↪.0.117232)
Summary Apache HTTP Server is prone to an out-of-bounds read vulnerability in mod_macro.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 2.4.52 Fixed version: 2.4.58 Installation path / port: /usr/sbin/apache2
Solution: Solution type: VendorFix Update to version 2.4.58 or later.
Affected Software/OS Apache HTTP Server version 2.4.57 and prior.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server < 2.4.58 'mod_macro' Out-of-bounds Read Vulnerability - Linux
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.100272 Version used: 2024-02-15T05:05:40Z
Product Detection Result Product: cpe:/a:apache:http_server:2.4.52 Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)
References cve: CVE-2023-31122 url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.58 url: https://www.openwall.com/lists/oss-security/2023/10/19/4 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0899 cert-bund: WID-SEC-2024-0869 cert-bund: WID-SEC-2024-0769 cert-bund: WID-SEC-2024-0107 cert-bund: WID-SEC-2023-2917 cert-bund: WID-SEC-2023-2712 dfn-cert: DFN-CERT-2024-1411 dfn-cert: DFN-CERT-2024-1010 dfn-cert: DFN-CERT-2024-1000 dfn-cert: DFN-CERT-2024-0732 dfn-cert: DFN-CERT-2023-2640 dfn-cert: DFN-CERT-2023-2583

High (CVSS: 7.5) NVT: SQLite 1.0.12 < 3.39.2 Improper Input Validation Vulnerability
Product detection result cpe:/a:sqlite:sqlite:3.37.2 Detected by SQLite Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.25623.1.0.↵113789)
Summary SQLite is prone to an improper input validation vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.37.2 Fixed version: 3.39.2 Installation path / port: /usr/bin/sqlite3
... continues on next page ...

...continued from previous page ...
Solution: Solution type: VendorFix Update to version 3.39.2 or later.
Affected Software/OS SQLite versions starting from 1.0.12 and before 3.39.2.
Vulnerability Insight SQLite sometimes allows an array-bounds overflow if billions of bytes are used in a string argument to a C API.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: SQLite 1.0.12 < 3.39.2 Improper Input Validation Vulnerability OID:1.3.6.1.4.1.25623.1.0.126102 Version used: 2023-10-19T05:05:21Z
Product Detection Result Product: cpe:/a:sqlite:sqlite:3.37.2 Method: SQLite Detection (Linux/Unix SSH Login) OID: 1.3.6.1.4.1.25623.1.0.113789)
References cve: CVE-2022-35737 url: https://www.sqlite.org/cves.html url: https://kb.cert.org/vuls/id/720344 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2024-0036 cert-bund: WID-SEC-2023-2229 cert-bund: WID-SEC-2023-1614 cert-bund: WID-SEC-2023-1542 cert-bund: WID-SEC-2023-1350 cert-bund: WID-SEC-2023-1021 cert-bund: WID-SEC-2023-0419 cert-bund: WID-SEC-2023-0138 cert-bund: WID-SEC-2022-2290 cert-bund: WID-SEC-2022-1972 cert-bund: WID-SEC-2022-1776 cert-bund: WID-SEC-2022-1766 dfn-cert: DFN-CERT-2024-0229 dfn-cert: DFN-CERT-2024-0055 dfn-cert: DFN-CERT-2023-1590 dfn-cert: DFN-CERT-2022-2472 dfn-cert: DFN-CERT-2022-2306
...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2022-2079
High (CVSS: 7.5) NVT: ISC BIND DoS Vulnerability (CVE-2024-11187) - Linux
Product detection result cpe:/a:isc:bind:9.18.30 Detected by ISC BIND Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145294)
Summary ISC BIND is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 9.18.30 Fixed version: 9.18.33 Installation path / port: /usr/sbin/named
Impact A named instance vulnerable to this issue can be compelled to consume excessive CPU resources up to the point where exhaustion of resources effectively prevents the server from responding to other client queries. This issue is most likely to affect resolvers but could also degrade authoritative server performance. - Authoritative servers are affected by this vulnerability. - Resolvers are affected by this vulnerability.
Solution: Solution type: VendorFix Update to version 9.18.33, 9.20.5, 9.21.4, 9.18.33-S1 or later.
Affected Software/OS ISC BIND version 9.11.37 and prior, 9.16.0 through 9.16.50, 9.18.0 through 9.18.32, 9.20.0 through 9.20.4, 9.21.0 through 9.21.3, 9.11.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.50-S1 and 9.18.11-S1 through 9.18.32-S1.
Vulnerability Insight It is possible to construct a zone such that some queries to it will generate responses containing numerous records in the Additional section. An attacker sending many such queries can cause either the authoritative server itself or an independent resolver to use disproportionate resources processing the queries. Zones will usually need to have been deliberately crafted to attack this exposure.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ISC BIND DoS Vulnerability (CVE-2024-11187) - Linux OID:1.3.6.1.4.1.25623.1.0.153891 Version used: 2025-01-31T05:37:27Z
Product Detection Result Product: cpe:/a:isc:bind:9.18.30 Method: ISC BIND Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145294)
References cve: CVE-2024-11187 url: https://kb.isc.org/docs/cve-2024-11187 cert-bund: WID-SEC-2025-0217 dfn-cert: DFN-CERT-2025-0300 dfn-cert: DFN-CERT-2025-0269
High (CVSS: 7.5) NVT: OpenSSL 1.1.1 < 1.1.1t, 3.0 < 3.0.8 DoS Vulnerability - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.8 Installation path / port: /usr/bin/openssl
Solution: Solution type: VendorFix Update to version 1.1.1t, 3.0.8 or later.
Affected Software/OS OpenSSL version 1.1.1 and 3.0.
... continues on next page ...

...continued from previous page...

Vulnerability Insight

The flaw exists due to a double free after calling PEM_read_bio_ex.

Vulnerability Detection Method

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

Details: OpenSSL 1.1.1 < 1.1.1t, 3.0 < 3.0.8 DoS Vulnerability - Linux

OID:1.3.6.1.4.1.25623.1.0.104535

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

Product Detection Result

Product: cpe:/a:openssl:openssl:3.0.2

Method: OpenSSL Detection Consolidation

OID: 1.3.6.1.4.1.25623.1.0.145462)

References

cve: CVE-2022-4450

url: <https://www.openssl.org/news/secadv/20230207.txt>

cert-bund: WID-SEC-2024-1591

cert-bund: WID-SEC-2024-0794

cert-bund: WID-SEC-2024-0114

cert-bund: WID-SEC-2023-1812

cert-bund: WID-SEC-2023-1432

cert-bund: WID-SEC-2023-1424

cert-bund: WID-SEC-2023-0304

dfn-cert: DFN-CERT-2024-1799

dfn-cert: DFN-CERT-2024-0147

dfn-cert: DFN-CERT-2024-0126

dfn-cert: DFN-CERT-2024-0016

dfn-cert: DFN-CERT-2023-1590

dfn-cert: DFN-CERT-2023-1423

dfn-cert: DFN-CERT-2023-1297

dfn-cert: DFN-CERT-2023-1256

dfn-cert: DFN-CERT-2023-1162

dfn-cert: DFN-CERT-2023-1043

dfn-cert: DFN-CERT-2023-0884

dfn-cert: DFN-CERT-2023-0661

dfn-cert: DFN-CERT-2023-0639

dfn-cert: DFN-CERT-2023-0618

dfn-cert: DFN-CERT-2023-0329

dfn-cert: DFN-CERT-2023-0318

dfn-cert: DFN-CERT-2023-0310

dfn-cert: DFN-CERT-2023-0299

dfn-cert: DFN-CERT-2023-0284

dfn-cert: DFN-CERT-2023-0283

High (CVSS: 7.5) NVT: OpenSSL 1.1.1 < 1.1.1t, 3.0 < 3.0.8 DoS Vulnerability - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.8 Installation path / port: /snap/core22/1748/usr/bin/openssl
Solution: Solution type: VendorFix Update to version 1.1.1t, 3.0.8 or later.
Affected Software/OS OpenSSL version 1.1.1 and 3.0.
Vulnerability Insight The flaw exists due to a double free after calling PEM_read_bio_ex.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL 1.1.1 < 1.1.1t, 3.0 < 3.0.8 DoS Vulnerability - Linux OID:1.3.6.1.4.1.25623.1.0.104535 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2022-4450 url: https://www.openssl.org/news/secadv/20230207.txt cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2024-0114
... continues on next page ...

...continued from previous page ...	
cert-bund:	WID-SEC-2023-1812
cert-bund:	WID-SEC-2023-1432
cert-bund:	WID-SEC-2023-1424
cert-bund:	WID-SEC-2023-0304
dfn-cert:	DFN-CERT-2024-1799
dfn-cert:	DFN-CERT-2024-0147
dfn-cert:	DFN-CERT-2024-0126
dfn-cert:	DFN-CERT-2024-0016
dfn-cert:	DFN-CERT-2023-1590
dfn-cert:	DFN-CERT-2023-1423
dfn-cert:	DFN-CERT-2023-1297
dfn-cert:	DFN-CERT-2023-1256
dfn-cert:	DFN-CERT-2023-1162
dfn-cert:	DFN-CERT-2023-1043
dfn-cert:	DFN-CERT-2023-0884
dfn-cert:	DFN-CERT-2023-0661
dfn-cert:	DFN-CERT-2023-0639
dfn-cert:	DFN-CERT-2023-0618
dfn-cert:	DFN-CERT-2023-0329
dfn-cert:	DFN-CERT-2023-0318
dfn-cert:	DFN-CERT-2023-0310
dfn-cert:	DFN-CERT-2023-0299
dfn-cert:	DFN-CERT-2023-0284
dfn-cert:	DFN-CERT-2023-0283

High (CVSS: 7.5)

NVT: OpenSSL 1.1.1 < 1.1.1t, 3.0 < 3.0.8 DoS Vulnerability - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

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

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 3.0.2

Fixed version: 3.0.8

Installation

path / port: /snap/core22/1612/usr/bin/openssl

Solution:

Solution type: VendorFix

Update to version 1.1.1t, 3.0.8 or later.

... continues on next page ...

...continued from previous page ...
Affected Software/OS OpenSSL version 1.1.1 and 3.0.
Vulnerability Insight The flaw exists due to a double free after calling PEM_read_bio_ex.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL 1.1.1 < 1.1.1t, 3.0 < 3.0.8 DoS Vulnerability - Linux OID:1.3.6.1.4.1.25623.1.0.104535 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2022-4450 url: https://www.openssl.org/news/secadv/20230207.txt cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2024-0114 cert-bund: WID-SEC-2023-1812 cert-bund: WID-SEC-2023-1432 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-0304 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-0147 dfn-cert: DFN-CERT-2024-0126 dfn-cert: DFN-CERT-2024-0016 dfn-cert: DFN-CERT-2023-1590 dfn-cert: DFN-CERT-2023-1423 dfn-cert: DFN-CERT-2023-1297 dfn-cert: DFN-CERT-2023-1256 dfn-cert: DFN-CERT-2023-1162 dfn-cert: DFN-CERT-2023-1043 dfn-cert: DFN-CERT-2023-0884 dfn-cert: DFN-CERT-2023-0661 dfn-cert: DFN-CERT-2023-0639 dfn-cert: DFN-CERT-2023-0618 dfn-cert: DFN-CERT-2023-0329 dfn-cert: DFN-CERT-2023-0318 dfn-cert: DFN-CERT-2023-0310
...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2023-0299
 dfn-cert: DFN-CERT-2023-0284
 dfn-cert: DFN-CERT-2023-0283

High (CVSS: 7.5)**NVT: OpenSSL: Multiple Vulnerabilities (Nov 2022) - Linux****Product detection result**

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 3.0.2

Fixed version: 3.0.7

Installation

path / port: /snap/core22/1612/usr/bin/openssl

Solution:**Solution type:** VendorFix

Update to version 3.0.7 or later.

Affected Software/OS

OpenSSL versions 3.0.0 through 3.0.6.

Vulnerability Insight

The following vulnerabilities exist:

- CVE-2022-3602: X.509 Email Address 4-byte Buffer Overflow
- CVE-2022-3786: X.509 Email Address Variable Length Buffer Overflow

Vulnerability Detection Method

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

Details: OpenSSL: Multiple Vulnerabilities (Nov 2022) - Linux

OID:1.3.6.1.4.1.25623.1.0.104416

Version used: 2023-10-19T05:05:21Z

Product Detection Result

Product: cpe:/a:openssl:openssl:3.0.2

Method: OpenSSL Detection Consolidation

OID: 1.3.6.1.4.1.25623.1.0.145462)

... continues on next page ...

...continued from previous page ...

References

cve: CVE-2022-3602
 cve: CVE-2022-3786
 url: <https://www.openssl.org/news/secadv/20221101.txt>
 url: <https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/>
 cert-bund: WID-SEC-2023-1969
 cert-bund: WID-SEC-2023-0561
 cert-bund: WID-SEC-2022-1922
 dfn-cert: DFN-CERT-2023-1839
 dfn-cert: DFN-CERT-2022-2898
 dfn-cert: DFN-CERT-2022-2601
 dfn-cert: DFN-CERT-2022-2478
 dfn-cert: DFN-CERT-2022-2444
 dfn-cert: DFN-CERT-2022-2441

High (CVSS: 7.5)

NVT: ISC BIND DoS Vulnerability (CVE-2024-12705) - Linux

Product detection result

cpe:/a:isc:bind:9.18.30
 Detected by ISC BIND Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145294)

Summary

ISC BIND is prone to a denial of service (DoS) vulnerability in the DNS-over-HTTPS implementation.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 9.18.30
 Fixed version: 9.18.33
 Installation
 path / port: /usr/sbin/named

Impact

By flooding a target resolver with HTTP/2 traffic and exploiting this flaw, an attacker could overwhelm the server, causing high CPU and/or memory usage and preventing other clients from establishing DoH connections. This would significantly impair the resolver's performance and effectively deny legitimate clients access to the DNS resolution service.

- Authoritative servers are affected by this vulnerability.
- Resolvers are affected by this vulnerability.

Solution:**Solution type:** VendorFix

Update to version 9.18.33, 9.20.5, 9.21.4, 9.18.33-S1 or later.

... continues on next page ...

...continued from previous page ...
Affected Software/OS ISC BIND version 9.18.0 through 9.18.32, 9.20.0 through 9.20.4, 9.21.0 through 9.21.3 and 9.18.11-S1 through 9.18.32-S1.
Vulnerability Insight Clients using DNS-over-HTTPS (DoH) can exhaust a DNS resolver's CPU and/or memory by flooding it with crafted valid or invalid HTTP/2 traffic.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ISC BIND DoS Vulnerability (CVE-2024-12705) - Linux OID:1.3.6.1.4.1.25623.1.0.153893 Version used: 2025-01-31T05:37:27Z
Product Detection Result Product: cpe:/a:isc:bind:9.18.30 Method: ISC BIND Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145294)
References cve: CVE-2024-12705 url: https://kb.isc.org/docs/cve-2024-12705 cert-bund: WID-SEC-2025-0217 dfn-cert: DFN-CERT-2025-0269

High (CVSS: 7.5) NVT: Apache HTTP Server < 2.4.59 Multiple Vulnerabilities - Linux
Product detection result cpe:/a:apache:http_server:2.4.52 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1 ↪.0.117232)
Summary Apache HTTP Server is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 2.4.52 Fixed version: 2.4.59 Installation
... continues on next page ...

...continued from previous page ...	
path / port:	/usr/sbin/apache2
Solution: Solution type: VendorFix Update to version 2.4.59 or later.	
Affected Software/OS Apache HTTP Server version 2.4.58 and prior.	
Vulnerability Insight The following vulnerabilities exist: - CVE-2023-38709: HTTP response splitting - CVE-2024-24795: HTTP response splitting in multiple modules - CVE-2024-27316: HTTP/2 DoS by memory exhaustion on endless continuation frames	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server < 2.4.59 Multiple Vulnerabilities - Linux OID:1.3.6.1.4.1.25623.1.0.152039 Version used: 2024-06-07T05:05:42Z	
Product Detection Result Product: cpe:/a:apache:http_server:2.4.52 Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)	
References cve: CVE-2023-38709 cve: CVE-2024-24795 cve: CVE-2024-27316 url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.59 url: https://kb.cert.org/vuls/id/421644 url: https://nowotarski.info/http2-continuation-flood/ url: https://nowotarski.info/http2-continuation-flood-technical-details/ cert-bund: WID-SEC-2024-1725 cert-bund: WID-SEC-2024-1643 cert-bund: WID-SEC-2024-1642 cert-bund: WID-SEC-2024-1504 cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0801 cert-bund: WID-SEC-2024-0789 dfn-cert: DFN-CERT-2024-2900 dfn-cert: DFN-CERT-2024-2534 dfn-cert: DFN-CERT-2024-2076	
... continues on next page ...	

...continued from previous page ...
dfn-cert: DFN-CERT-2024-1958
dfn-cert: DFN-CERT-2024-1853
dfn-cert: DFN-CERT-2024-1749
dfn-cert: DFN-CERT-2024-1697
dfn-cert: DFN-CERT-2024-1411
dfn-cert: DFN-CERT-2024-1335
dfn-cert: DFN-CERT-2024-1238
dfn-cert: DFN-CERT-2024-1031
dfn-cert: DFN-CERT-2024-1010
dfn-cert: DFN-CERT-2024-0964
dfn-cert: DFN-CERT-2024-0901
dfn-cert: DFN-CERT-2024-0890

High (CVSS: 7.5) NVT: OpenSSL: X.509 Policy Constraints Double Locking Vulnerability (Dec 2022) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.8 Installation path / port: /snap/core22/1748/usr/bin/openssl
Solution: Solution type: VendorFix Update to version 3.0.8 or later.
Affected Software/OS OpenSSL versions 3.0.0 through 3.0.7.
Vulnerability Insight If an X.509 certificate contains a malformed policy constraint and policy processing is enabled, then a write lock will be taken twice recursively. On some operating systems (most widely: Windows) this results in a denial of service when the affected process hangs. Policy processing being enabled on a publicly facing server is not considered to be a common setup.
... continues on next page ...

...continued from previous page ...	
Policy processing is enabled by passing the '-policy' argument to the command line utilities or by calling either 'X509_VERIFY_PARAM_add0_policy()' or 'X509_VERIFY_PARAM_set1_policies()' functions.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL: X.509 Policy Constraints Double Locking Vulnerability (Dec 2022) - Lin. ↪.. OID:1.3.6.1.4.1.25623.1.0.149016 Version used: 2023-10-19T05:05:21Z	
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)	
References cve: CVE-2022-3996 url: https://www.openssl.org/news/secadv/20221213.txt cert-bund: WID-SEC-2022-2310 dfn-cert: DFN-CERT-2023-0960 dfn-cert: DFN-CERT-2023-0661 dfn-cert: DFN-CERT-2023-0639 dfn-cert: DFN-CERT-2022-2898 dfn-cert: DFN-CERT-2022-2831	

High (CVSS: 7.5) NVT: OpenSSL: X.509 Policy Constraints Double Locking Vulnerability (Dec 2022) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.8 Installation path / port: /snap/core22/1612/usr/bin/openssl
Solution:
... continues on next page ...

...continued from previous page ...	
Solution type: VendorFix Update to version 3.0.8 or later.	
Affected Software/OS OpenSSL versions 3.0.0 through 3.0.7.	
Vulnerability Insight If an X.509 certificate contains a malformed policy constraint and policy processing is enabled, then a write lock will be taken twice recursively. On some operating systems (most widely: Windows) this results in a denial of service when the affected process hangs. Policy processing being enabled on a publicly facing server is not considered to be a common setup. Policy processing is enabled by passing the '-policy' argument to the command line utilities or by calling either 'X509_VERIFY_PARAM_add0_policy()' or 'X509_VERIFY_PARAM_set1_policies()' functions.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL: X.509 Policy Constraints Double Locking Vulnerability (Dec 2022) - Lin. ↔.. OID:1.3.6.1.4.1.25623.1.0.149016 Version used: 2023-10-19T05:05:21Z	
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)	
References cve: CVE-2022-3996 url: https://www.openssl.org/news/secadv/20221213.txt cert-bund: WID-SEC-2022-2310 dfn-cert: DFN-CERT-2023-0960 dfn-cert: DFN-CERT-2023-0661 dfn-cert: DFN-CERT-2023-0639 dfn-cert: DFN-CERT-2022-2898 dfn-cert: DFN-CERT-2022-2831	
High (CVSS: 7.5) NVT: OpenSSL Multiple Vulnerabilities (20230322, 20230328, 20230530) - Linux	
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)	
... continues on next page ...	

...continued from previous page ...
Summary OpenSSL is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.9 Installation path / port: /snap/core22/1612/usr/bin/openssl
Solution: Solution type: VendorFix Update to version 1.0.2zh, 1.1.1u, 3.0.9, 3.1.1 or later.
Affected Software/OS OpenSSL version 1.0.2, 1.1.1, 3.0 and 3.1.
Vulnerability Insight The following flaws exist: - CVE-2023-0464: Excessive Resource Usage Verifying X.509 Policy Constraints - CVE-2023-0465: Invalid certificate policies in leaf certificates are silently ignored - CVE-2023-0466: Certificate policy check not enabled - CVE-2023-2650: Possible DoS translating ASN.1 object identifiers
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL Multiple Vulnerabilities (20230322, 20230328, 20230530) - Linux OID: 1.3.6.1.4.1.25623.1.0.104655 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2023-0464 cve: CVE-2023-0465 cve: CVE-2023-0466 cve: CVE-2023-2650 url: https://www.openssl.org/news/secadv/20230322.txt url: https://www.openssl.org/news/secadv/20230328.txt url: https://www.openssl.org/news/secadv/20230530.txt
... continues on next page ...

...continued from previous page...

cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0120
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2024-0053
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2690
cert-bund: WID-SEC-2023-2674
cert-bund: WID-SEC-2023-1794
cert-bund: WID-SEC-2023-1781
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-1323
cert-bund: WID-SEC-2023-1130
cert-bund: WID-SEC-2023-0782
cert-bund: WID-SEC-2023-0732
dfn-cert: DFN-CERT-2024-1799
dfn-cert: DFN-CERT-2024-1067
dfn-cert: DFN-CERT-2024-0565
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2024-0125
dfn-cert: DFN-CERT-2023-3071
dfn-cert: DFN-CERT-2023-3070
dfn-cert: DFN-CERT-2023-2749
dfn-cert: DFN-CERT-2023-2545
dfn-cert: DFN-CERT-2023-2536
dfn-cert: DFN-CERT-2023-2116
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1903
dfn-cert: DFN-CERT-2023-1720
dfn-cert: DFN-CERT-2023-1649
dfn-cert: DFN-CERT-2023-1642
dfn-cert: DFN-CERT-2023-1462
dfn-cert: DFN-CERT-2023-1428
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1332
dfn-cert: DFN-CERT-2023-1246
dfn-cert: DFN-CERT-2023-1245
dfn-cert: DFN-CERT-2023-1233
dfn-cert: DFN-CERT-2023-0999
dfn-cert: DFN-CERT-2023-0960
dfn-cert: DFN-CERT-2023-0904
dfn-cert: DFN-CERT-2023-0782
dfn-cert: DFN-CERT-2023-0700
dfn-cert: DFN-CERT-2023-0645

<p>High (CVSS: 7.5) NVT: PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 NULL Deference Vulnerability (Feb 2021) - Linux</p>
<p>Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>Summary PHP is prone to a NULL dereference vulnerability in the SoapClient.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.3.27 Installation path / port: /usr/bin/php7.2</p>
<p>Solution: Solution type: VendorFix Update to version 7.3.27, 7.4.15, 8.0.2 or later.</p>
<p>Affected Software/OS PHP versions prior to 7.3.27, 7.4.x prior to 7.4.15 and 8.0.x prior to 8.0.2.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 NULL Deference Vulnerability (Feb 2021) - Linux ↪.. OID:1.3.6.1.4.1.25623.1.0.145323 Version used: 2021-11-29T15:00:35Z</p>
<p>Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>References cve: CVE-2021-21702 url: https://www.php.net/ChangeLog-7.php#7.3.27 url: https://www.php.net/ChangeLog-7.php#7.4.15 url: https://www.php.net/ChangeLog-8.php#8.0.2 cert-bund: WID-SEC-2023-1737 cert-bund: WID-SEC-2022-2113</p>
<p>... continues on next page ...</p>

cert-bund: CB-K21/0124	...continued from previous page ...
dfn-cert: DFN-CERT-2023-1600	
dfn-cert: DFN-CERT-2022-2639	
dfn-cert: DFN-CERT-2022-2638	
dfn-cert: DFN-CERT-2022-0904	
dfn-cert: DFN-CERT-2021-2373	
dfn-cert: DFN-CERT-2021-1645	
dfn-cert: DFN-CERT-2021-1509	
dfn-cert: DFN-CERT-2021-1453	
dfn-cert: DFN-CERT-2021-0556	
dfn-cert: DFN-CERT-2021-0380	
dfn-cert: DFN-CERT-2021-0246	

High (CVSS: 7.5)

NVT: PHP 'CVE-2017-7189' Improper Input Validation Vulnerability - Linux

Product detection result

cpe:/a:php:php:7.2.34

Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

PHP is improperly validating input from untrusted input.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 7.2.34

Fixed version: None

Installation

path / port: /usr/bin/php7.2

Solution:

Solution type: WillNotFix

No solution was made available by the vendor. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Note: PHP versions 7.0.18 and 7.1.4 introduced a fix which was reverted again in version 7.0.19 / 7.1.5 respectively and the fix wasn't introduced again as of today (08-2020).

Affected Software/OS

All PHP versions since 4.3.0 up to the latest 7.x versions.

Note: PHP versions 7.0.18 and 7.1.4 introduced a fix which was reverted again in version 7.0.19 / 7.1.5 respectively.

Vulnerability Insight

... continues on next page ...

...continued from previous page ...
main/streams/xp_socket.c in PHP misparses fsockopen calls, such as by interpreting fsockopen('127.0.0.1:80', 443) as if the address/port were 127.0.0.1:80:443, which is later truncated to 127.0.0.1:80. This behavior has a security risk if the explicitly provided port number (i.e., 443 in this example) is hardcoded into an application as a security policy, but the hostname argument (i.e., 127.0.0.1:80 in this example) is obtained from untrusted input.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP 'CVE-2017-7189' Improper Input Validation Vulnerability - Linux OID:1.3.6.1.4.1.25623.1.0.108874 Version used: 2024-02-15T05:05:40Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2017-7189 url: https://bugs.php.net/bug.php?id=74192 url: https://bugs.php.net/bug.php?id=74429 url: https://github.com/php/php-src/commit/bab0b99f376dac9170ac81382a5ed526938d5c95a

High (CVSS: 7.5) NVT: OpenSSL Multiple Vulnerabilities (20230322, 20230328, 20230530) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.9 Installation path / port: /snap/core22/1748/usr/bin/openssl
Solution: Solution type: VendorFix Update to version 1.0.2zh, 1.1.1u, 3.0.9, 3.1.1 or later.
... continues on next page ...

...continued from previous page ...
Affected Software/OS OpenSSL version 1.0.2, 1.1.1, 3.0 and 3.1.
Vulnerability Insight The following flaws exist: - CVE-2023-0464: Excessive Resource Usage Verifying X.509 Policy Constraints - CVE-2023-0465: Invalid certificate policies in leaf certificates are silently ignored - CVE-2023-0466: Certificate policy check not enabled - CVE-2023-2650: Possible DoS translating ASN.1 object identifiers
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL Multiple Vulnerabilities (20230322, 20230328, 20230530) - Linux OID:1.3.6.1.4.1.25623.1.0.104655 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2023-0464 cve: CVE-2023-0465 cve: CVE-2023-0466 cve: CVE-2023-2650 url: https://www.openssl.org/news/secadv/20230322.txt url: https://www.openssl.org/news/secadv/20230328.txt url: https://www.openssl.org/news/secadv/20230530.txt cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2024-0120 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2024-0053 cert-bund: WID-SEC-2023-2917 cert-bund: WID-SEC-2023-2690 cert-bund: WID-SEC-2023-2674 cert-bund: WID-SEC-2023-1794 cert-bund: WID-SEC-2023-1781 cert-bund: WID-SEC-2023-1614 cert-bund: WID-SEC-2023-1432 cert-bund: WID-SEC-2023-1323 cert-bund: WID-SEC-2023-1130 cert-bund: WID-SEC-2023-0782
... continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2023-0732 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-1067 dfn-cert: DFN-CERT-2024-0565 dfn-cert: DFN-CERT-2024-0147 dfn-cert: DFN-CERT-2024-0125 dfn-cert: DFN-CERT-2023-3071 dfn-cert: DFN-CERT-2023-3070 dfn-cert: DFN-CERT-2023-2749 dfn-cert: DFN-CERT-2023-2545 dfn-cert: DFN-CERT-2023-2536 dfn-cert: DFN-CERT-2023-2116 dfn-cert: DFN-CERT-2023-1947 dfn-cert: DFN-CERT-2023-1903 dfn-cert: DFN-CERT-2023-1720 dfn-cert: DFN-CERT-2023-1649 dfn-cert: DFN-CERT-2023-1642 dfn-cert: DFN-CERT-2023-1462 dfn-cert: DFN-CERT-2023-1428 dfn-cert: DFN-CERT-2023-1423 dfn-cert: DFN-CERT-2023-1332 dfn-cert: DFN-CERT-2023-1246 dfn-cert: DFN-CERT-2023-1245 dfn-cert: DFN-CERT-2023-1233 dfn-cert: DFN-CERT-2023-0999 dfn-cert: DFN-CERT-2023-0960 dfn-cert: DFN-CERT-2023-0904 dfn-cert: DFN-CERT-2023-0782 dfn-cert: DFN-CERT-2023-0700 dfn-cert: DFN-CERT-2023-0645

High (CVSS: 7.5) NVT: Mozilla Firefox Security Advisory (MFSA2024-46) - Linux
Product detection result cpe:/a:mozilla:firefox:136.0 Detected by Mozilla Firefox Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.2 ↪5623.1.0.800017)
Summary This host is missing a security update for Mozilla Firefox.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 130.0
... continues on next page ...

...continued from previous page...	
Fixed version:	131
Installation path / port:	/snap/firefox/4848/usr/lib/firefox/firefox
Solution: Solution type: VendorFix The vendor has released an update. Please see the reference(s) for more information.	
Affected Software/OS Firefox version(s) below 131.	
Vulnerability Insight CVE-2024-9392: Compromised content process can bypass site isolation A compromised content process could have allowed for the arbitrary loading of cross-origin pages. CVE-2024-9393: Cross-origin access to PDF contents through multipart responses An attacker could, via a specially crafted multipart response, execute arbitrary JavaScript under the resource://pdf.js origin. This could allow them to access cross-origin PDF content. This access is limited to 'same site' documents by the Site Isolation feature on desktop clients, but full cross-origin access is possible on Android versions. CVE-2024-9394: Cross-origin access to JSON contents through multipart responses An attacker could, via a specially crafted multipart response, execute arbitrary JavaScript under the resource://devtools origin. This could allow them to access cross-origin JSON content. This access is limited to 'same site' documents by the Site Isolation feature on desktop clients, but full cross-origin access is possible on Android versions. CVE-2024-9396: Potential memory corruption may occur when cloning certain objects It is currently unknown if this issue is exploitable but a condition may arise where the structured clone of certain objects could lead to memory corruption. CVE-2024-9397: Potential directory upload bypass via clickjacking A missing delay in directory upload UI could have made it possible for an attacker to trick a user into granting permission via clickjacking. CVE-2024-9398: External protocol handlers could be enumerated via popups By checking the result of calls to window.open with specifically set protocol handlers, an attacker could determine if the application which implements that protocol handler is installed. CVE-2024-9399: Specially crafted WebTransport requests could lead to denial of service A web-site configured to initiate a specially crafted WebTransport session could crash the Firefox process leading to a denial of service condition. CVE-2024-9400: Potential memory corruption during JIT compilation A potential memory corruption vulnerability could be triggered if an attacker had the ability to trigger an OOM at a specific moment during JIT compilation. CVE-2024-9401: Memory safety bugs ... [Please see the references for more information on the vulnerabilities]	
Vulnerability Detection Method Checks if a vulnerable package version is present on the target host. Details: Mozilla Firefox Security Advisory (MFSa2024-46) - Linux OID:1.3.6.1.4.1.25623.1.2.1.2024.46	
...continues on next page...	

...continued from previous page...	
Version used: 2024-10-16T08:00:45Z	
Product Detection Result Product: cpe:/a:mozilla:firefox:136.0 Method: Mozilla Firefox Detection (Linux/Unix SSH Login) OID: 1.3.6.1.4.1.25623.1.0.800017)	
References cve: CVE-2024-9392 cve: CVE-2024-9393 cve: CVE-2024-9394 cve: CVE-2024-9396 cve: CVE-2024-9397 cve: CVE-2024-9398 cve: CVE-2024-9399 cve: CVE-2024-9400 cve: CVE-2024-9401 cve: CVE-2024-9402 cve: CVE-2024-9403 advisory-id: MFSa2024-46 url: https://www.mozilla.org/en-US/security/advisories/mfsa2024-46/ url: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1872744%2C1897792%2C1911317%2C1913445%2C1914106%2C1914475%2C1914963%2C1915008%2C1916476 url: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1872744%2C1897792%2C1911317%2C1916476 url: https://bugzilla.mozilla.org/show_bug.cgi?id=1881037 url: https://bugzilla.mozilla.org/show_bug.cgi?id=1899154 url: https://bugzilla.mozilla.org/show_bug.cgi?id=1905843 url: https://bugzilla.mozilla.org/show_bug.cgi?id=1907726 url: https://bugzilla.mozilla.org/show_bug.cgi?id=1912471 url: https://bugzilla.mozilla.org/show_bug.cgi?id=1915249 url: https://bugzilla.mozilla.org/show_bug.cgi?id=1916659 url: https://bugzilla.mozilla.org/show_bug.cgi?id=1917807 url: https://bugzilla.mozilla.org/show_bug.cgi?id=1918301 url: https://bugzilla.mozilla.org/show_bug.cgi?id=1918874 cert-bund: WID-SEC-2024-3057 dfn-cert: DFN-CERT-2025-0030 dfn-cert: DFN-CERT-2024-3152 dfn-cert: DFN-CERT-2024-2761 dfn-cert: DFN-CERT-2024-2694 dfn-cert: DFN-CERT-2024-2594 dfn-cert: DFN-CERT-2024-2593	

High (CVSS: 7.5) NVT: OpenSSL Multiple Vulnerabilities (20230322, 20230328, 20230530) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.9 Installation path / port: /usr/bin/openssl
Solution: Solution type: VendorFix Update to version 1.0.2zh, 1.1.1u, 3.0.9, 3.1.1 or later.
Affected Software/OS OpenSSL version 1.0.2, 1.1.1, 3.0 and 3.1.
Vulnerability Insight The following flaws exist: <ul style="list-style-type: none"> - CVE-2023-0464: Excessive Resource Usage Verifying X.509 Policy Constraints - CVE-2023-0465: Invalid certificate policies in leaf certificates are silently ignored - CVE-2023-0466: Certificate policy check not enabled - CVE-2023-2650: Possible DoS translating ASN.1 object identifiers
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL Multiple Vulnerabilities (20230322, 20230328, 20230530) - Linux OID:1.3.6.1.4.1.25623.1.0.104655 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2023-0464
... continues on next page ...

...continued from previous page ...

cve: CVE-2023-0465
cve: CVE-2023-0466
cve: CVE-2023-2650
url: <https://www.openssl.org/news/secadv/20230322.txt>
url: <https://www.openssl.org/news/secadv/20230328.txt>
url: <https://www.openssl.org/news/secadv/20230530.txt>
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0120
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2024-0053
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2690
cert-bund: WID-SEC-2023-2674
cert-bund: WID-SEC-2023-1794
cert-bund: WID-SEC-2023-1781
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-1323
cert-bund: WID-SEC-2023-1130
cert-bund: WID-SEC-2023-0782
cert-bund: WID-SEC-2023-0732
dfn-cert: DFN-CERT-2024-1799
dfn-cert: DFN-CERT-2024-1067
dfn-cert: DFN-CERT-2024-0565
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2024-0125
dfn-cert: DFN-CERT-2023-3071
dfn-cert: DFN-CERT-2023-3070
dfn-cert: DFN-CERT-2023-2749
dfn-cert: DFN-CERT-2023-2545
dfn-cert: DFN-CERT-2023-2536
dfn-cert: DFN-CERT-2023-2116
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1903
dfn-cert: DFN-CERT-2023-1720
dfn-cert: DFN-CERT-2023-1649
dfn-cert: DFN-CERT-2023-1642
dfn-cert: DFN-CERT-2023-1462
dfn-cert: DFN-CERT-2023-1428
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1332
dfn-cert: DFN-CERT-2023-1246
dfn-cert: DFN-CERT-2023-1245
dfn-cert: DFN-CERT-2023-1233
dfn-cert: DFN-CERT-2023-0999
dfn-cert: DFN-CERT-2023-0960

... continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2023-0904
dfn-cert: DFN-CERT-2023-0782
dfn-cert: DFN-CERT-2023-0700
dfn-cert: DFN-CERT-2023-0645

High (CVSS: 7.5) NVT: Apache HTTP Server 2.4.30 - 2.4.55 HTTP Request Smuggling Vulnerability - Linux
Product detection result cpe:/a:apache:http_server:2.4.52 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1 ↔.0.117232)
Summary Apache HTTP Server is prone to a HTTP request smuggling vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 2.4.52 Fixed version: 2.4.56 Installation path / port: /usr/sbin/apache2
Solution: Solution type: VendorFix Update to version 2.4.56 or later.
Affected Software/OS Apache HTTP Server versions 2.4.30 through 2.4.55.
Vulnerability Insight HTTP Response Smuggling vulnerability via mod_proxy_uwsgi. Special characters in the origin response header can truncate/split the response forwarded to the client.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server 2.4.30 - 2.4.55 HTTP Request Smuggling Vulnerability - Linux OID:1.3.6.1.4.1.25623.1.0.104599 Version used: 2024-02-15T05:05:40Z
Product Detection Result Product: cpe:/a:apache:http_server:2.4.52 ... continues on next page ...

Linux

...continued from previous page ...
Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)
References cve: CVE-2023-27522 url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.56 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2023-2031 cert-bund: WID-SEC-2023-1424 cert-bund: WID-SEC-2023-0583 dfn-cert: DFN-CERT-2024-1808 dfn-cert: DFN-CERT-2023-1895 dfn-cert: DFN-CERT-2023-0658 dfn-cert: DFN-CERT-2023-0546

High (CVSS: 7.5) NVT: Mozilla Firefox Security Advisory (MFSA2024-63) - Linux
Product detection result cpe:/a:mozilla:firefox:136.0 Detected by Mozilla Firefox Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.2 ↔5623.1.0.800017)
Summary This host is missing a security update for Mozilla Firefox.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 130.0 Fixed version: 133 Installation path / port: /snap/firefox/4848/usr/lib/firefox/firefox
Solution: Solution type: VendorFix The vendor has released an update. Please see the reference(s) for more information.
Affected Software/OS Firefox version(s) below 133.
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
<p>CVE-2024-11692: Select list elements could be shown over another site An attacker could cause a select dropdown to be shown over another tab, this could have led to user confusion and possible spoofing attacks.</p> <p>CVE-2024-11701: Misleading Address Bar State During Navigation Interruption The incorrect domain may have been displayed in the address bar during an interrupted navigation attempt. This could have led to user confusion and possible spoofing attacks.</p> <p>CVE-2024-11694: CSP Bypass and XSS Exposure via Web Compatibility Shims Enhanced Tracking Protection's Strict mode may have inadvertently allowed a CSP frame-src bypass and DOM-based XSS through the Google SafeFrame shim in the Web Compatibility extension. This issue could have exposed users to malicious frames masquerading as legitimate content.</p> <p>CVE-2024-11695: URL Bar Spoofing via Manipulated Punycode and Whitespace Characters A crafted URL containing Arabic script and whitespace characters could have hidden the true origin of the page, resulting in a potential spoofing attack.</p> <p>CVE-2024-11696: Unhandled Exception in Add-on Signature Verification The application failed to account for exceptions thrown by the loadManifestFromFile method during add-on signature verification. This flaw, triggered by an invalid or unsupported extension manifest, could have caused runtime errors that disrupted the signature validation process. As a result, the enforcement of signature validation for unrelated add-ons may have been bypassed. Signature validation in this context is used to ensure that third-party applications on the user's ... [Please see the references for more information on the vulnerabilities]</p>
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable package version is present on the target host.</p> <p>Details: Mozilla Firefox Security Advisory (MFSa2024-63) - Linux</p> <p>OID:1.3.6.1.4.1.25623.1.2.1.2024.63</p> <p>Version used: 2025-01-09T06:16:22Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:mozilla:firefox:136.0</p> <p>Method: Mozilla Firefox Detection (Linux/Unix SSH Login)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.800017)</p>
<p>References</p> <p>cve: CVE-2024-11692</p> <p>cve: CVE-2024-11694</p> <p>cve: CVE-2024-11695</p> <p>cve: CVE-2024-11696</p> <p>cve: CVE-2024-11697</p> <p>cve: CVE-2024-11699</p> <p>cve: CVE-2024-11701</p> <p>cve: CVE-2024-11704</p> <p>cve: CVE-2024-11705</p> <p>cve: CVE-2024-11706</p> <p>cve: CVE-2024-11708</p> <p>advisory-id: MFSa2024-63</p> <p>url: https://www.mozilla.org/en-US/security/advisories/mfsa2024-63/</p>
...continues on next page ...

...continued from previous page ...
url: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1880582%2C1929911
url: https://bugzilla.mozilla.org/show_bug.cgi?id=1842187
url: https://bugzilla.mozilla.org/show_bug.cgi?id=1899402
url: https://bugzilla.mozilla.org/show_bug.cgi?id=1909535
url: https://bugzilla.mozilla.org/show_bug.cgi?id=1914797
url: https://bugzilla.mozilla.org/show_bug.cgi?id=1921768
url: https://bugzilla.mozilla.org/show_bug.cgi?id=1922912
url: https://bugzilla.mozilla.org/show_bug.cgi?id=1923767
url: https://bugzilla.mozilla.org/show_bug.cgi?id=1924167
url: https://bugzilla.mozilla.org/show_bug.cgi?id=1925496
url: https://bugzilla.mozilla.org/show_bug.cgi?id=1929600
cert-bund: WID-SEC-2025-0262
cert-bund: WID-SEC-2024-3549
dfn-cert: DFN-CERT-2025-0306
dfn-cert: DFN-CERT-2025-0304
dfn-cert: DFN-CERT-2025-0030
dfn-cert: DFN-CERT-2024-3274
dfn-cert: DFN-CERT-2024-3151
dfn-cert: DFN-CERT-2024-3149

High (CVSS: 7.5) NVT: Mozilla Firefox Security Advisory (MFSA2025-01) - Linux
Product detection result cpe:/a:mozilla:firefox:136.0 Detected by Mozilla Firefox Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.2↵5623.1.0.800017)
Summary This host is missing a security update for Mozilla Firefox.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 130.0 Fixed version: 134 Installation path / port: /snap/firefox/4848/usr/lib/firefox/firefox
Solution: Solution type: VendorFix The vendor has released an update. Please see the reference(s) for more information.
Affected Software/OS ... continues on next page ...

...continued from previous page ...
Firefox version(s) below 134.
<p>Vulnerability Insight</p> <p>CVE-2025-0245: Lock screen setting bypass in Firefox Focus for Android Under certain circumstances, a user opt-in setting that Focus should require authentication before use could have been be bypassed.</p> <p>CVE-2025-0237: WebChannel APIs susceptible to confused deputy attack The WebChannel API, which is used to transport various information across processes, did not check the sending principal but rather accepted the principal being sent. This could have led to privilege escalation attacks.</p> <p>CVE-2025-0238: Use-after-free when breaking lines in text Assuming a controlled failed memory allocation, an attacker could have caused a use-after-free, leading to a potentially exploitable crash.</p> <p>CVE-2025-0239: Alt-Svc ALPN validation failure when redirected When using Alt-Svc, ALPN did not properly validate certificates when the original server is redirecting to an insecure site.</p> <p>CVE-2025-0240: Compartment mismatch when parsing JavaScript JSON module Parsing a JavaScript module as JSON could, under some circumstances, cause cross-compartment access, which may result in a use-after-free.</p> <p>CVE-2025-0241: Memory corruption when using JavaScript Text Segmentation When segmenting specially crafted text, segmentation would corrupt memory leading to a potentially exploitable crash.</p> <p>CVE-2025-0242: Memory safety bugs fixed in Firefox 134, Thunderbird 134, Firefox ESR 115.19, Firefox ESR 128.6, Thunderbird 115.19, and Thunderbird 128.6 Memory safety bugs present in Firefox 133, Thunderbird 133, Firefox ESR 115.18, Firefox ESR 128.5, Thunderbird 115.18, and Thunderbird 128.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code.</p> <p>CVE-2025-0243: Memory safety bugs fixed in Firefox 134, Thunderbird 134, Firefox ESR 128.6, and Thunderbird 128.6 Memory safety bugs present in Firefox 133, Thunderbird 133, Firefox ESR 128.5, and Thunderbird 128.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code.</p> <p>CVE-2025-0247: Memory safety bugs fixed in Firefox 134 and Thunderbird 134 Memory safety bugs present in Firefox 133 and Thunderbird 133. Some of these bugs showed evidence of memory corruption and ... [Please see the references for more information on the vulnerabilities]</p>
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable package version is present on the target host.</p> <p>Details: Mozilla Firefox Security Advisory (MFSa2025-01) - Linux</p> <p>OID:1.3.6.1.4.1.25623.1.2.1.2025.01</p> <p>Version used: 2025-01-09T06:16:22Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:mozilla:firefox:136.0</p> <p>Method: Mozilla Firefox Detection (Linux/Unix SSH Login)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.800017)</p>
... continues on next page ...

...continued from previous page ...

References

cve: CVE-2025-0237
 cve: CVE-2025-0238
 cve: CVE-2025-0239
 cve: CVE-2025-0240
 cve: CVE-2025-0241
 cve: CVE-2025-0242
 cve: CVE-2025-0243
 cve: CVE-2025-0245
 cve: CVE-2025-0247
 advisory-id: MFSa2025-01
 url: <https://www.mozilla.org/en-US/security/advisories/mfsa2025-01/>
 url: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1827142%2C1932783
 url: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1835193%2C1910021%2C1919803%2C1931576%2C1931948%2C1932173
 url: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1874523%2C1926454%2C1931873%2C1932169
 url: https://bugzilla.mozilla.org/show_bug.cgi?id=1895342
 url: https://bugzilla.mozilla.org/show_bug.cgi?id=1915257
 url: https://bugzilla.mozilla.org/show_bug.cgi?id=1915535
 url: https://bugzilla.mozilla.org/show_bug.cgi?id=1929156
 url: https://bugzilla.mozilla.org/show_bug.cgi?id=1929623
 url: https://bugzilla.mozilla.org/show_bug.cgi?id=1933023
 cert-bund: WID-SEC-2025-0026
 dfn-cert: DFN-CERT-2025-0047
 dfn-cert: DFN-CERT-2025-0030
 dfn-cert: DFN-CERT-2025-0023

High (CVSS: 7.5)

NVT: OpenSSL: Multiple Vulnerabilities (Nov 2022) - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 3.0.2

Fixed version: 3.0.7

Installation

path / port: /snap/core22/1748/usr/bin/openssl

... continues on next page ...

...continued from previous page ...
Solution: Solution type: VendorFix Update to version 3.0.7 or later.
Affected Software/OS OpenSSL versions 3.0.0 through 3.0.6.
Vulnerability Insight The following vulnerabilities exist: - CVE-2022-3602: X.509 Email Address 4-byte Buffer Overflow - CVE-2022-3786: X.509 Email Address Variable Length Buffer Overflow
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL: Multiple Vulnerabilities (Nov 2022) - Linux OID: 1.3.6.1.4.1.25623.1.0.104416 Version used: 2023-10-19T05:05:21Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2022-3602 cve: CVE-2022-3786 url: https://www.openssl.org/news/secadv/20221101.txt url: https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/ cert-bund: WID-SEC-2023-1969 cert-bund: WID-SEC-2023-0561 cert-bund: WID-SEC-2022-1922 dfn-cert: DFN-CERT-2023-1839 dfn-cert: DFN-CERT-2022-2898 dfn-cert: DFN-CERT-2022-2601 dfn-cert: DFN-CERT-2022-2478 dfn-cert: DFN-CERT-2022-2444 dfn-cert: DFN-CERT-2022-2441
High (CVSS: 7.5) NVT: OpenSSL Incorrect Cipher Key & IV Length Processing Vulnerability (20231024) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
... continues on next page ...

...continued from previous page ...
Summary OpenSSL is prone to an incorrect processing of key and initialisation vector (IV) lengths vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.12 Installation path / port: /snap/core22/1612/usr/bin/openssl
Impact A truncation in the IV can result in non-uniqueness, which could result in loss of confidentiality for some cipher modes.
Solution: Solution type: VendorFix Update to version 3.0.12, 3.1.4 or later.
Affected Software/OS OpenSSL version 3.0 and 3.1.
Vulnerability Insight When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() or EVP_CipherInit_ex2() the provided OSSL_PARAM array is processed after the key and IV have been established. Any alterations to the key length, via the 'keylen' parameter or the IV length, via the 'ivlen' parameter, within the OSSL_PARAM array will not take effect as intended, potentially causing truncation or overreading of these values. The following ciphers and cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL Incorrect Cipher Key & IV Length Processing Vulnerability (20231024) - . ↪.. OID:1.3.6.1.4.1.25623.1.0.170621 Version used: 2023-11-10T16:09:31Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
...continues on next page ...

...continued from previous page ...

References

cve: CVE-2023-5363
 url: <https://www.openssl.org/news/secadv/20231024.txt>
 url: <https://www.openssl.org/news/vulnerabilities-3.0.html#CVE-2023-5363>
 url: <https://www.openssl.org/news/vulnerabilities-3.1.html#CVE-2023-5363>
 cert-bund: WID-SEC-2024-1591
 cert-bund: WID-SEC-2024-1488
 cert-bund: WID-SEC-2024-1248
 cert-bund: WID-SEC-2024-0869
 cert-bund: WID-SEC-2024-0119
 cert-bund: WID-SEC-2023-3032
 cert-bund: WID-SEC-2023-2741
 dfn-cert: DFN-CERT-2024-1799
 dfn-cert: DFN-CERT-2024-1601
 dfn-cert: DFN-CERT-2024-1413
 dfn-cert: DFN-CERT-2024-1067
 dfn-cert: DFN-CERT-2024-0744
 dfn-cert: DFN-CERT-2024-0491
 dfn-cert: DFN-CERT-2024-0285
 dfn-cert: DFN-CERT-2024-0253
 dfn-cert: DFN-CERT-2024-0191
 dfn-cert: DFN-CERT-2024-0127
 dfn-cert: DFN-CERT-2023-2624
 dfn-cert: DFN-CERT-2023-2615
 dfn-cert: DFN-CERT-2023-2610

High (CVSS: 7.5)**NVT: OpenSSL: Multiple Vulnerabilities (Nov 2022) - Linux****Product detection result**

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 3.0.2

Fixed version: 3.0.7

Installation

path / port: /usr/bin/openssl

Solution:**Solution type:** VendorFix

... continues on next page ...

...continued from previous page ...
Update to version 3.0.7 or later.
Affected Software/OS OpenSSL versions 3.0.0 through 3.0.6.
Vulnerability Insight The following vulnerabilities exist: - CVE-2022-3602: X.509 Email Address 4-byte Buffer Overflow - CVE-2022-3786: X.509 Email Address Variable Length Buffer Overflow
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: <code>OpenSSL: Multiple Vulnerabilities (Nov 2022) - Linux</code> OID: 1.3.6.1.4.1.25623.1.0.104416 Version used: 2023-10-19T05:05:21Z
Product Detection Result Product: <code>cpe:/a:openssl:openssl:3.0.2</code> Method: <code>OpenSSL Detection Consolidation</code> OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2022-3602 cve: CVE-2022-3786 url: https://www.openssl.org/news/secadv/20221101.txt url: https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/ cert-bund: WID-SEC-2023-1969 cert-bund: WID-SEC-2023-0561 cert-bund: WID-SEC-2022-1922 dfn-cert: DFN-CERT-2023-1839 dfn-cert: DFN-CERT-2022-2898 dfn-cert: DFN-CERT-2022-2601 dfn-cert: DFN-CERT-2022-2478 dfn-cert: DFN-CERT-2022-2444 dfn-cert: DFN-CERT-2022-2441

High (CVSS: 7.5)

NVT: `OpenSSL Incorrect Cipher Key & IV Length Processing Vulnerability (20231024) - Linux`

Product detection result

`cpe:/a:openssl:openssl:3.0.2`

Detected by `OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)`

Summary

... continues on next page ...

...continued from previous page ...
OpenSSL is prone to an incorrect processing of key and initialisation vector (IV) lengths vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.12 Installation path / port: /snap/core22/1748/usr/bin/openssl
Impact A truncation in the IV can result in non-uniqueness, which could result in loss of confidentiality for some cipher modes.
Solution: Solution type: VendorFix Update to version 3.0.12, 3.1.4 or later.
Affected Software/OS OpenSSL version 3.0 and 3.1.
Vulnerability Insight When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() or EVP_CipherInit_ex2() the provided OSSL_PARAM array is processed after the key and IV have been established. Any alterations to the key length, via the 'keylen' parameter or the IV length, via the 'ivlen' parameter, within the OSSL_PARAM array will not take effect as intended, potentially causing truncation or overreading of these values. The following ciphers and cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL Incorrect Cipher Key & IV Length Processing Vulnerability (20231024) - . ↪.. OID:1.3.6.1.4.1.25623.1.0.170621 Version used: 2023-11-10T16:09:31Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2023-5363 url: https://www.openssl.org/news/secadv/20231024.txt
... continues on next page ...

...continued from previous page ...
url: https://www.openssl.org/news/vulnerabilities-3.0.html#CVE-2023-5363
url: https://www.openssl.org/news/vulnerabilities-3.1.html#CVE-2023-5363
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-1488
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-0869
cert-bund: WID-SEC-2024-0119
cert-bund: WID-SEC-2023-3032
cert-bund: WID-SEC-2023-2741
dfn-cert: DFN-CERT-2024-1799
dfn-cert: DFN-CERT-2024-1601
dfn-cert: DFN-CERT-2024-1413
dfn-cert: DFN-CERT-2024-1067
dfn-cert: DFN-CERT-2024-0744
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0285
dfn-cert: DFN-CERT-2024-0253
dfn-cert: DFN-CERT-2024-0191
dfn-cert: DFN-CERT-2024-0127
dfn-cert: DFN-CERT-2023-2624
dfn-cert: DFN-CERT-2023-2615
dfn-cert: DFN-CERT-2023-2610

High (CVSS: 7.5)

NVT: OpenSSL Incorrect Cipher Key & IV Length Processing Vulnerability (20231024) - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to an incorrect processing of key and initialisation vector (IV) lengths vulnerability.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 3.0.2

Fixed version: 3.0.12

Installation

path / port: /usr/bin/openssl

Impact

A truncation in the IV can result in non-uniqueness, which could result in loss of confidentiality for some cipher modes.

... continues on next page ...

...continued from previous page ...
Solution: Solution type: VendorFix Update to version 3.0.12, 3.1.4 or later.
Affected Software/OS OpenSSL version 3.0 and 3.1.
Vulnerability Insight When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() or EVP_CipherInit_ex2() the provided OSSL_PARAM array is processed after the key and IV have been established. Any alterations to the key length, via the 'keylen' parameter or the IV length, via the 'ivlen' parameter, within the OSSL_PARAM array will not take effect as intended, potentially causing truncation or overreading of these values. The following ciphers and cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL Incorrect Cipher Key & IV Length Processing Vulnerability (20231024) - . ↔.. OID:1.3.6.1.4.1.25623.1.0.170621 Version used: 2023-11-10T16:09:31Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2023-5363 url: https://www.openssl.org/news/secadv/20231024.txt url: https://www.openssl.org/news/vulnerabilities-3.0.html#CVE-2023-5363 url: https://www.openssl.org/news/vulnerabilities-3.1.html#CVE-2023-5363 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-1488 cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2024-0869 cert-bund: WID-SEC-2024-0119 cert-bund: WID-SEC-2023-3032 cert-bund: WID-SEC-2023-2741 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-1601 dfn-cert: DFN-CERT-2024-1413 dfn-cert: DFN-CERT-2024-1067 dfn-cert: DFN-CERT-2024-0744
...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0285
dfn-cert: DFN-CERT-2024-0253
dfn-cert: DFN-CERT-2024-0191
dfn-cert: DFN-CERT-2024-0127
dfn-cert: DFN-CERT-2023-2624
dfn-cert: DFN-CERT-2023-2615
dfn-cert: DFN-CERT-2023-2610

High (CVSS: 7.3) NVT: SQLite < 3.43.1 Buffer Overflow Vulnerability
Product detection result cpe:/a:sqlite:sqlite:3.37.2 Detected by SQLite Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.25623.1.0.↪113789)
Summary SQLite is prone to a buffer overflow vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.37.2 Fixed version: 3.43.1 Installation path / port: /usr/bin/sqlite3
Solution: Solution type: VendorFix Update to version 3.43.1 or later.
Affected Software/OS SQLite prior to version 3.43.1.
Vulnerability Insight This issue affects the function sessionReadRecord of the file ext/session/sqlite3session.c of the component make alltest Handler. The manipulation leads to heap-based buffer overflow.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: SQLite < 3.43.1 Buffer Overflow Vulnerability OID:1.3.6.1.4.1.25623.1.0.126572 Version used: 2024-06-26T05:05:39Z
... continues on next page ...

...continued from previous page ...
Product Detection Result Product: cpe:/a:sqlite:sqlite:3.37.2 Method: SQLite Detection (Linux/Unix SSH Login) OID: 1.3.6.1.4.1.25623.1.0.113789)
References cve: CVE-2023-7104 url: https://sqlite.org/forum/forumpost/5bcbf4571c cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-0521 cert-bund: WID-SEC-2024-0092 dfn-cert: DFN-CERT-2024-2579 dfn-cert: DFN-CERT-2024-1413 dfn-cert: DFN-CERT-2024-1102 dfn-cert: DFN-CERT-2024-0791 dfn-cert: DFN-CERT-2024-0744 dfn-cert: DFN-CERT-2024-0115 dfn-cert: DFN-CERT-2024-0030 dfn-cert: DFN-CERT-2024-0020

High (CVSS: 7.3) NVT: SQLite 3.37.0 - 3.40.0 Information Disclosure Vulnerability
Product detection result cpe:/a:sqlite:sqlite:3.37.2 Detected by SQLite Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.25623.1.0.↵113789)
Summary SQLite is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.37.2 Fixed version: 3.40.1 Installation path / port: /usr/bin/sqlite3
Solution: Solution type: VendorFix Update to version 3.40.1 or later.
... continues on next page ...

...continued from previous page ...
Affected Software/OS SQLite versions 3.37.0 through 3.40.0.
Vulnerability Insight When relying on <code>--safe</code> flag, execution of an untrusted CLI script, does not properly implement the <code>azProhibitedFunctions</code> protection mechanism, and instead allows UDF functions such as <code>WRITEFILE</code> .
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: SQLite 3.37.0 - 3.40.0 Information Disclosure Vulnerability OID:1.3.6.1.4.1.25623.1.0.126250 Version used: 2023-12-14T05:05:32Z
Product Detection Result Product: <code>cpe:/a:sqlite:sqlite:3.37.2</code> Method: SQLite Detection (Linux/Unix SSH Login) OID: 1.3.6.1.4.1.25623.1.0.113789)
References cve: CVE-2022-46908 url: https://sqlite.org/forum/forumpost/07beac8056151b2f cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2024-0119 cert-bund: WID-SEC-2023-2031 cert-bund: WID-SEC-2023-1728 cert-bund: WID-SEC-2023-1614 cert-bund: WID-SEC-2023-1022 cert-bund: WID-SEC-2023-1017 cert-bund: WID-SEC-2023-1016 dfn-cert: DFN-CERT-2024-0127 dfn-cert: DFN-CERT-2024-0020 dfn-cert: DFN-CERT-2023-1230 dfn-cert: DFN-CERT-2023-0881 dfn-cert: DFN-CERT-2022-2904
High (CVSS: 7.2) NVT: LibreOffice Improper Certificate Validation Vulnerability (Aug 2024) - Linux
Product detection result <code>cpe:/a:libreoffice:libreoffice:7.3.7.2.2</code> Detected by LibreOffice Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.25623 ↪.1.0.902701)
... continues on next page ...

...continued from previous page ...
Summary LibreOffice is prone to an improper certificate validation vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.3.7.2.2 Fixed version: 24.2.5 Installation path / port: /usr/bin/libreoffice
Impact Successful exploitation allows an attacker to compromise the affected system.
Solution: Solution type: VendorFix Update to version 24.2.5 or later.
Affected Software/OS LibreOffice version before 24.2.5 on Linux.
Vulnerability Insight The flaw exists when handling documents with signed macros inside.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: LibreOffice Improper Certificate Validation Vulnerability (Aug 2024) - Linux OID:1.3.6.1.4.1.25623.1.0.834295 Version used: 2024-10-18T15:39:59Z
Product Detection Result Product: cpe:/a:libreoffice:libreoffice:7.3.7.2.2 Method: LibreOffice Detection (Linux/Unix SSH Login) OID: 1.3.6.1.4.1.25623.1.0.902701)
References cve: CVE-2024-6472 url: https://www.libreoffice.org/about-us/security/advisories/CVE-2024-6472 url: https://www.cybersecurity-help.cz/vdb/SB20240805107 cert-bund: WID-SEC-2024-1764 dfn-cert: DFN-CERT-2024-2003

<p>High (CVSS: 7.0) NVT: PHP 5.3.7 - 7.3.31, 7.4.x < 7.4.25, 8.0.x < 8.0.12 Security Update (Oct 2021) - Linux</p>
<p>Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>Summary PHP released new versions which includes a security fix.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.3.32 (not released yet) Installation path / port: /usr/bin/php7.2</p>
<p>Solution: Solution type: VendorFix Update to version 7.3.32 (not released yet), 7.4.25, 8.0.12 or later.</p>
<p>Affected Software/OS PHP versions 5.3.7 through 7.3.31, 7.4.x through 7.4.24 and 8.0.x through 8.0.11. Note: While the referenced CVE is only listing PHP 7.3.x, 7.4.x and 8.0.x as affected the security research team is stating in the linked blog post that all versions down to 5.3.7 are affected.</p>
<p>Vulnerability Insight Fixed bug #81026 (PHP-FPM oob R/W in root process leading to privilege escalation).</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP 5.3.7 - 7.3.31, 7.4.x < 7.4.25, 8.0.x < 8.0.12 Security Update (Oct 2021) -. ↪.. OID:1.3.6.1.4.1.25623.1.0.117752 Version used: 2021-11-05T03:03:34Z</p>
<p>Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>References cve: CVE-2021-21703 url: https://www.php.net/ChangeLog-7.php#7.3.32 ... continues on next page ...</p>

...continued from previous page ...

```

url: https://www.php.net/ChangeLog-7.php#7.4.25
url: https://www.php.net/ChangeLog-8.php#8.0.12
url: http://bugs.php.net/81026
url: https://www.ambionics.io/blog/php-fpm-local-root
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2022-0624
cert-bund: WID-SEC-2022-0586
cert-bund: CB-K21/1106
dfn-cert: DFN-CERT-2023-1600
dfn-cert: DFN-CERT-2022-2639
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2022-2337
dfn-cert: DFN-CERT-2022-1493
dfn-cert: DFN-CERT-2022-1046
dfn-cert: DFN-CERT-2022-0485
dfn-cert: DFN-CERT-2021-2586
dfn-cert: DFN-CERT-2021-2474
dfn-cert: DFN-CERT-2021-2200

```

[\[return to 10.0.0.92 \]](#)

2.2.4 High 22/tcp

High (CVSS: 9.8)**NVT: OpenBSD OpenSSH 8.9 - 9.2 Unspecified Vulnerability****Product detection result**

cpe:/a:openbsd:openssh:8.9p1

Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

Summary

OpenBSD OpenSSH is prone to an unspecified vulnerability.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 8.9p1

Fixed version: 9.3

Installation

path / port: 22/tcp

Solution:**Solution type:** VendorFix

Update to version 9.3 or later.

... continues on next page ...

...continued from previous page ...
Affected Software/OS OpenBSD OpenSSH versions starting from 8.9 and prior to 9.3.
Vulnerability Insight ssh-add(1): when adding smartcard keys to ssh-agent(1) with the per-hop destination constraints (ssh-add -h ...) added in OpenSSH 8.9, a logic error prevented the constraints from being communicated to the agent. This resulted in the keys being added without constraints. The common cases of non-smartcard keys and keys without destination constraints are unaffected. This problem was reported by Luci Stanescu.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH 8.9 - 9.2 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104634 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2023-28531 url: https://www.openssh.com/releases.html#9.3 url: https://www.openwall.com/lists/oss-security/2023/03/15/8 cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2023-0670 dfn-cert: DFN-CERT-2024-1260 dfn-cert: DFN-CERT-2024-0341 dfn-cert: DFN-CERT-2023-3218 dfn-cert: DFN-CERT-2023-3182 dfn-cert: DFN-CERT-2023-1424
High (CVSS: 9.8) NVT: OpenBSD OpenSSH < 9.3p2 RCE Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to a remote code execution (RCE) vulnerability in OpenSSH's forwarded ssh-agent.
... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.3p2 Installation path / port: 22/tcp
Solution: Solution type: VendorFix Update to version 9.3p2 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.3p2. The following conditions needs to be met: - Exploitation requires the presence of specific libraries on the victim system. - Remote exploitation requires that the agent was forwarded to an attacker-controlled system.
Vulnerability Insight A condition where specific libraries loaded via ssh-agent(1)'s PKCS#11 support could be abused to achieve remote code execution via a forwarded agent socket.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.3p2 RCE Vulnerability OID:1.3.6.1.4.1.25623.1.0.104869 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2023-38408 url: https://www.openssh.com/releases/notes.html#9.3p2 url: https://www.qualys.com/2023/07/19/cve-2023-38408/rce-openssh-forwarded-ssh-agent.txt cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2023-2679 cert-bund: WID-SEC-2023-2625
... continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2023-2240
cert-bund: WID-SEC-2023-1843
cert-bund: WID-SEC-2023-1819
dfn-cert: DFN-CERT-2024-1260
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2023-2792
dfn-cert: DFN-CERT-2023-2179
dfn-cert: DFN-CERT-2023-1961
dfn-cert: DFN-CERT-2023-1920
dfn-cert: DFN-CERT-2023-1845
dfn-cert: DFN-CERT-2023-1773
dfn-cert: DFN-CERT-2023-1665

High (CVSS: 8.1) NVT: OpenBSD OpenSSH < 4.4p1, 8.5p1 - 9.7p1 RCE Vulnerability (regreSSHion)
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to a remote code execution (RCE) vulnerability dubbed 'regreSSH-ion'.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.8 Installation path / port: 22/tcp
Solution: Solution type: VendorFix Update to version 9.8 or later.
Affected Software/OS OpenBSD OpenSSH versions prior to 4.4p1 (unless patched for CVE-2006-5051 and CVE-2008-4109) and 8.5p1 through 9.7p1.
Vulnerability Insight Vendor insights: 1) Race condition in sshd(8) A critical vulnerability in sshd(8) was present that may allow arbitrary code execution with root privileges.
... continues on next page ...

<p>...continued from previous page ...</p> <p>Successful exploitation has been demonstrated on 32-bit Linux/glibc systems with ASLR. Under lab conditions, the attack requires on average 6-8 hours of continuous connections up to the maximum the server will accept. Exploitation on 64-bit systems is believed to be possible but has not been demonstrated at this time. It's likely that these attacks will be improved upon. Exploitation on non-glibc systems is conceivable but has not been examined. Systems that lack ASLR or users of downstream Linux distributions that have modified OpenSSH to disable per-connection ASLR re-randomisation (yes - this is a thing, no - we don't understand why) may potentially have an easier path to exploitation. OpenBSD is not vulnerable.</p>
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: OpenBSD OpenSSH < 4.4p1, 8.5p1 - 9.7p1 RCE Vulnerability (regreSSHion)</p> <p>OID:1.3.6.1.4.1.25623.1.0.114680</p> <p>Version used: 2024-07-09T05:05:54Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:openbsd:openssh:8.9p1</p> <p>Method: OpenSSH Detection Consolidation</p> <p>OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>References</p> <p>cve: CVE-2024-6387</p> <p>url: https://www.openssh.com/txt/release-9.8</p> <p>url: https://www.openssh.com/security.html</p> <p>url: https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt</p> <p>url: https://www.qualys.com/regresshion-cve-2024-6387/</p> <p>url: https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server</p> <p>url: https://unit42.paloaltonetworks.com/threat-brief-cve-2024-6387-openssh/</p> <p>cert-bund: WID-SEC-2024-3195</p> <p>cert-bund: WID-SEC-2024-1725</p> <p>cert-bund: WID-SEC-2024-1486</p> <p>dfn-cert: DFN-CERT-2025-0042</p> <p>dfn-cert: DFN-CERT-2024-1960</p> <p>dfn-cert: DFN-CERT-2024-1959</p> <p>dfn-cert: DFN-CERT-2024-1958</p> <p>dfn-cert: DFN-CERT-2024-1904</p> <p>dfn-cert: DFN-CERT-2024-1869</p> <p>dfn-cert: DFN-CERT-2024-1868</p> <p>dfn-cert: DFN-CERT-2024-1844</p> <p>dfn-cert: DFN-CERT-2024-1759</p> <p>dfn-cert: DFN-CERT-2024-1740</p> <p>dfn-cert: DFN-CERT-2024-1694</p> <p>dfn-cert: DFN-CERT-2024-1693</p>

<p>High (CVSS: 7.5) NVT: Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)</p>
<p>Product detection result cpe:/a:ietf:secure_shell_protocol Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↔)</p>
<p>Summary The remote SSH server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange (KEX) algorithms and thus could be prone to a denial of service (DoS) vulnerability.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result The remote SSH server supports the following DHE KEX algorithm(s): diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha256</p>
<p>Impact This vulnerability allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, also known as a D(HE)ater attack. There could be an increase in CPU usage in the affected component. For OpenSSH, users may observe issues such as a slowdown in SSH connections.</p>
<p>Solution: Solution type: Mitigation - DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.</p>
<p>Vulnerability Insight - CVE-2002-20001: The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.</p>
<p>... continues on next page ...</p>

<p>...continued from previous page ...</p> <p>- CVE-2022-40735: The Diffie-Hellman Key Agreement Protocol allows use of long exponents that arguably make certain calculations unnecessarily expensive, because the 1996 van Oorschot and Wiener paper found that '(appropriately) short exponents' can be used when there are adequate subgroup constraints, and these short exponents can lead to less expensive calculations than for long exponents. This issue is different from CVE-2002-20001 because it is based on an observation about exponent size, rather than an observation about numbers that are not public keys. The specific situations in which calculation expense would constitute a server-side vulnerability depend on the protocol (e.g., TLS, SSH, or IKE) and the DHE implementation details. In general, there might be an availability concern because of server-side resource consumption from DHE modular-exponentiation calculations. Finally, it is possible for an attacker to exploit this vulnerability and CVE-2002-20001 together.</p> <p>- CVE-2024-41996: Validating the order of the public keys in the Diffie-Hellman Key Agreement Protocol, when an approved safe prime is used, allows remote attackers (from the client side) to trigger unnecessarily expensive server-side DHE modular-exponentiation calculations. The client may cause asymmetric resource consumption. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE and validate the order of the public key.</p>
<p>Vulnerability Detection Method Checks the supported KEX algorithms of the remote SSH server. Details: Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater) OID:1.3.6.1.4.1.25623.1.0.117839 Version used: 2024-10-03T05:05:33Z</p>
<p>Product Detection Result Product: cpe:/a:ietf:secure_shell_protocol Method: SSH Protocol Algorithms Supported OID: 1.3.6.1.4.1.25623.1.0.105565)</p>
<p>References cve: CVE-2002-20001 cve: CVE-2022-40735 cve: CVE-2024-41996 url: https://dheatattack.gitlab.io/ url: https://dheatattack.gitlab.io/details/ url: https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol url: https://github.com/Balasys/dheater url: https://github.com/c0r0n3r/dheater cert-bund: WID-SEC-2024-3056 cert-bund: WID-SEC-2023-1886 cert-bund: WID-SEC-2023-1352 cert-bund: WID-SEC-2022-2251 cert-bund: WID-SEC-2022-2000 cert-bund: CB-K22/0224 cert-bund: CB-K21/1276</p>
<p>...continues on next page ...</p>

...continued from previous page ...
dfn-cert: DFN-CERT-2024-2847
dfn-cert: DFN-CERT-2024-2578
dfn-cert: DFN-CERT-2024-1671
dfn-cert: DFN-CERT-2023-1697
dfn-cert: DFN-CERT-2023-1332
dfn-cert: DFN-CERT-2022-2147
dfn-cert: DFN-CERT-2022-0437
dfn-cert: DFN-CERT-2021-2622

[\[return to 10.0.0.92 \]](#)

2.2.5 High 53/tcp

High (CVSS: 7.5) NVT: ISC BIND DoS Vulnerability (CVE-2024-11187) - Linux
Product detection result cpe:/a:isc:bind:9.18.30 Detected by ISC BIND Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145294)
Summary ISC BIND is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 9.18.30 Fixed version: 9.18.33 Installation path / port: 53/tcp
Impact A named instance vulnerable to this issue can be compelled to consume excessive CPU resources up to the point where exhaustion of resources effectively prevents the server from responding to other client queries. This issue is most likely to affect resolvers but could also degrade authoritative server performance. - Authoritative servers are affected by this vulnerability. - Resolvers are affected by this vulnerability.
Solution: Solution type: VendorFix Update to version 9.18.33, 9.20.5, 9.21.4, 9.18.33-S1 or later.
Affected Software/OS ... continues on next page ...

...continued from previous page ...
ISC BIND version 9.11.37 and prior, 9.16.0 through 9.16.50, 9.18.0 through 9.18.32, 9.20.0 through 9.20.4, 9.21.0 through 9.21.3, 9.11.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.50-S1 and 9.18.11-S1 through 9.18.32-S1.
Vulnerability Insight It is possible to construct a zone such that some queries to it will generate responses containing numerous records in the Additional section. An attacker sending many such queries can cause either the authoritative server itself or an independent resolver to use disproportionate resources processing the queries. Zones will usually need to have been deliberately crafted to attack this exposure.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ISC BIND DoS Vulnerability (CVE-2024-11187) - Linux OID:1.3.6.1.4.1.25623.1.0.153891 Version used: 2025-01-31T05:37:27Z
Product Detection Result Product: cpe:/a:isc:bind:9.18.30 Method: ISC BIND Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145294)
References cve: CVE-2024-11187 url: https://kb.isc.org/docs/cve-2024-11187 cert-bund: WID-SEC-2025-0217 dfn-cert: DFN-CERT-2025-0300 dfn-cert: DFN-CERT-2025-0269

High (CVSS: 7.5) NVT: ISC BIND DoS Vulnerability (CVE-2024-12705) - Linux
Product detection result cpe:/a:isc:bind:9.18.30 Detected by ISC BIND Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145294)
Summary ISC BIND is prone to a denial of service (DoS) vulnerability in the DNS-over-HTTPS implementation.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 9.18.30 Fixed version: 9.18.33
... continues on next page ...

...continued from previous page...	
Installation	
path / port:	53/tcp
Impact	<p>By flooding a target resolver with HTTP/2 traffic and exploiting this flaw, an attacker could overwhelm the server, causing high CPU and/or memory usage and preventing other clients from establishing DoH connections. This would significantly impair the resolver's performance and effectively deny legitimate clients access to the DNS resolution service.</p> <ul style="list-style-type: none">- Authoritative servers are affected by this vulnerability.- Resolvers are affected by this vulnerability.
Solution:	
Solution type:	VendorFix
	Update to version 9.18.33, 9.20.5, 9.21.4, 9.18.33-S1 or later.
Affected Software/OS	
	ISC BIND version 9.18.0 through 9.18.32, 9.20.0 through 9.20.4, 9.21.0 through 9.21.3 and 9.18.11-S1 through 9.18.32-S1.
Vulnerability Insight	
	Clients using DNS-over-HTTPS (DoH) can exhaust a DNS resolver's CPU and/or memory by flooding it with crafted valid or invalid HTTP/2 traffic.
Vulnerability Detection Method	
	<p>Checks if a vulnerable version is present on the target host.</p> <p>Details: ISC BIND DoS Vulnerability (CVE-2024-12705) - Linux</p> <p>OID:1.3.6.1.4.1.25623.1.0.153893</p> <p>Version used: 2025-01-31T05:37:27Z</p>
Product Detection Result	
	<p>Product: cpe:/a:isc:bind:9.18.30</p> <p>Method: ISC BIND Detection Consolidation</p> <p>OID: 1.3.6.1.4.1.25623.1.0.145294)</p>
References	
	<p>cve: CVE-2024-12705</p> <p>url: https://kb.isc.org/docs/cve-2024-12705</p> <p>cert-bund: WID-SEC-2025-0217</p> <p>dfn-cert: DFN-CERT-2025-0269</p>

[\[return to 10.0.0.92 \]](#)

2.2.6 Medium 80/tcp

<p>Medium (CVSS: 6.5) NVT: PHP < 7.3.31, 7.4.x < 7.4.24, 8.0.x < 8.0.11 Security Update (Sep 2021) - Linux</p>
<p>Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>Summary PHP released new versions which includes a security fix.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.3.31 Installation path / port: 80/tcp</p>
<p>Solution: Solution type: VendorFix Update to version 7.3.31, 7.4.24, 8.0.11 or later.</p>
<p>Affected Software/OS PHP versions prior to 7.3.31, 7.4.x through 7.4.23 and 8.0.x through 8.0.10.</p>
<p>Vulnerability Insight Fixed bug #81420 (ZipArchive::extractTo extracts outside of destination).</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.3.31, 7.4.x < 7.4.24, 8.0.x < 8.0.11 Security Update (Sep 2021) - Linux OID:1.3.6.1.4.1.25623.1.0.117694 Version used: 2021-10-11T08:01:31Z</p>
<p>Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>References cve: CVE-2021-21706 url: https://www.php.net/ChangeLog-7.php#7.3.31 url: https://www.php.net/ChangeLog-7.php#7.4.24 url: https://www.php.net/ChangeLog-8.php#8.0.11 url: http://bugs.php.net/81420 ... continues on next page ...</p>

...continued from previous page ...
cert-bund: WID-SEC-2022-2112 cert-bund: CB-K21/1008 dfn-cert: DFN-CERT-2022-2639 dfn-cert: DFN-CERT-2021-2474 dfn-cert: DFN-CERT-2021-1994
Medium (CVSS: 6.5) NVT: PHP < 7.4.31, 8.0.x < 8.0.24, 8.1.x < 8.1.11 Security Update - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.4.31 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 7.4.31, 8.0.24, 8.1.11 or later.
Affected Software/OS PHP versions prior to 7.4.31, 8.0.x prior to 8.0.24 and 8.1.x prior to 8.1.11.
Vulnerability Insight The following vulnerabilities exist: - CVE-2022-31628: The phar uncompressor code would recursively uncompress 'quines' gzip files, resulting in an infinite loop. - CVE-2022-31629: The vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a '__Host-' or '__Secure-' cookie by PHP applications.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.4.31, 8.0.x < 8.0.24, 8.1.x < 8.1.11 Security Update - Linux OID:1.3.6.1.4.1.25623.1.0.104331 Version used: 2023-10-19T05:05:21Z
... continues on next page ...

...continued from previous page ...

Product Detection Result

Product: cpe:/a:php:php:7.2.34

Method: PHP Detection (HTTP)

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

cve: CVE-2022-31628

cve: CVE-2022-31629

url: <https://www.php.net/ChangeLog-7.php#7.4.31>url: <https://www.php.net/ChangeLog-8.php#8.0.24>url: <https://www.php.net/ChangeLog-8.php#8.1.11>url: <https://bugs.php.net/bug.php?id=81726>url: <https://bugs.php.net/bug.php?id=81727>

cert-bund: WID-SEC-2023-1737

cert-bund: WID-SEC-2023-0561

cert-bund: WID-SEC-2023-0137

cert-bund: WID-SEC-2022-1567

dfn-cert: DFN-CERT-2024-1192

dfn-cert: DFN-CERT-2023-1600

dfn-cert: DFN-CERT-2023-0422

dfn-cert: DFN-CERT-2022-2869

dfn-cert: DFN-CERT-2022-2639

dfn-cert: DFN-CERT-2022-2638

dfn-cert: DFN-CERT-2022-2598

dfn-cert: DFN-CERT-2022-2523

dfn-cert: DFN-CERT-2022-2337

dfn-cert: DFN-CERT-2022-2157

Medium (CVSS: 5.9)

NVT: PHP < 7.3.29 Multiple Vulnerabilities (Jul 2021) - Linux

Product detection result

cpe:/a:php:php:7.2.34

Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

PHP is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 7.2.34

Fixed version: 7.3.29

Installation

... continues on next page ...

...continued from previous page...	
path / port:	80/tcp
Solution: Solution type: VendorFix Update to version 7.3.29 or later.	
Affected Software/OS PHP versions prior to 7.3.29.	
Vulnerability Insight The following flaws exist: - CVE-2021-21705: SSRF bypass in FILTER_VALIDATE_URL. - CVE-2021-21704: Stack buffer overflow in firebird_info_cb. - CVE-2021-21704: SIGSEGV in firebird_handle_doer. - CVE-2021-21704: SIGSEGV in firebird_stmt_execute. - CVE-2021-21704: Crash while parsing blob data in firebird_fetch_blob.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.3.29 Multiple Vulnerabilities (Jul 2021) - Linux OID:1.3.6.1.4.1.25623.1.0.117524 Version used: 2023-10-20T16:09:12Z	
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)	
References cve: CVE-2021-21704 cve: CVE-2021-21705 url: https://www.php.net/ChangeLog-7.php#7.3.29 url: http://bugs.php.net/81122 url: http://bugs.php.net/76448 url: http://bugs.php.net/76449 url: http://bugs.php.net/76450 url: http://bugs.php.net/76452 cert-bund: WID-SEC-2023-1737 cert-bund: WID-SEC-2022-1577 cert-bund: WID-SEC-2022-0624 cert-bund: CB-K21/0705 dfn-cert: DFN-CERT-2023-1600 dfn-cert: DFN-CERT-2022-2639 dfn-cert: DFN-CERT-2022-2638 dfn-cert: DFN-CERT-2022-1046	
...continues on next page...	

...continued from previous page ...

```
dfn-cert: DFN-CERT-2021-2185
dfn-cert: DFN-CERT-2021-1676
dfn-cert: DFN-CERT-2021-1645
dfn-cert: DFN-CERT-2021-1627
dfn-cert: DFN-CERT-2021-1509
dfn-cert: DFN-CERT-2021-1453
dfn-cert: DFN-CERT-2021-1419
```

Medium (CVSS: 5.9)

NVT: Apache HTTP Server 2.4.17 - 2.4.57 DoS Vulnerability - Linux

Product detection result

cpe:/a:apache:http_server:2.4.52

Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↔.0.117232)**Summary**

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

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 2.4.52

Fixed version: 2.4.58

Installation

path / port: 80/tcp

Solution:**Solution type:** VendorFix

Update to version 2.4.58 or later.

Affected Software/OS

Apache HTTP Server version 2.4.17 through 2.4.57.

Vulnerability Insight

When a HTTP/2 stream was reset (RST frame) by a client, there was a time window where the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.

This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During 'normal' HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.

... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server 2.4.17 - 2.4.57 DoS Vulnerability - Linux OID:1.3.6.1.4.1.25623.1.0.100310 Version used: 2024-08-02T05:05:39Z
Product Detection Result Product: cpe:/a:apache:http_server:2.4.52 Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)
References cve: CVE-2023-45802 url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.58 url: https://www.openwall.com/lists/oss-security/2023/10/19/6 url: https://github.com/icing/blog/blob/main/h2-rapid-reset.md cert-bund: WID-SEC-2024-0769 cert-bund: WID-SEC-2023-2917 cert-bund: WID-SEC-2023-2712 dfn-cert: DFN-CERT-2024-2968 dfn-cert: DFN-CERT-2024-1411 dfn-cert: DFN-CERT-2024-1335 dfn-cert: DFN-CERT-2024-1152 dfn-cert: DFN-CERT-2024-1010 dfn-cert: DFN-CERT-2023-3071 dfn-cert: DFN-CERT-2023-2596 dfn-cert: DFN-CERT-2023-2583
Medium (CVSS: 5.8) NVT: PHP < 8.1.28, 8.2.x < 8.2.18, 8.3.x < 8.3.6 Security Update (GHSA-h746-cjrr-wfmr) - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to a vulnerability in password_verify.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 8.1.28 Installation
... continues on next page ...

...continued from previous page...	
path / port:	80/tcp
Solution: Solution type: VendorFix Update to version 8.1.28, 8.2.18, 8.3.6 or later.	
Affected Software/OS PHP prior to version 8.1.28, version 8.2.x through 8.2.17 and 8.3.x through 8.3.5.	
Vulnerability Insight If a password stored with password_hash starts with a null byte (\x00), testing a blank string as the password via password_verify will incorrectly return true. If a user were able to create a password with a leading null byte (unlikely, but syntactically valid), an attacker could trivially compromise the victim's account by attempting to sign in with a blank string.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 8.1.28, 8.2.x < 8.2.18, 8.3.x < 8.3.6 Security Update (GHSA-h746-cjrr-wfm. ↔.. OID:1.3.6.1.4.1.25623.1.0.152118 Version used: 2024-04-16T05:05:31Z	
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)	
References cve: CVE-2024-3096 url: https://github.com/php/php-src/security/advisories/GHSA-h746-cjrr-wfmr url: https://www.php.net/ChangeLog-8.php#8.1.28 url: https://www.php.net/ChangeLog-8.php#8.2.18 url: https://www.php.net/ChangeLog-8.php#8.3.6 cert-bund: WID-SEC-2024-0867 dfn-cert: DFN-CERT-2024-3330 dfn-cert: DFN-CERT-2024-3329 dfn-cert: DFN-CERT-2024-1574 dfn-cert: DFN-CERT-2024-1192 dfn-cert: DFN-CERT-2024-1132 dfn-cert: DFN-CERT-2024-1115 dfn-cert: DFN-CERT-2024-0993 dfn-cert: DFN-CERT-2024-0962	

<p>Medium (CVSS: 5.5) NVT: PHP < 8.0.22, 8.1.x < 8.1.9 Security Update - Linux</p>
<p>Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>Summary PHP is prone to a buffer overflow vulnerability.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 8.0.22/8.1.9/8.2.0 Installation path / port: 80/tcp</p>
<p>Solution: Solution type: VendorFix Update to version 8.0.22, 8.1.9, 8.2.0 or later.</p>
<p>Affected Software/OS PHP versions prior to 8.0.22 and 8.1.x prior to 8.1.9.</p>
<p>Vulnerability Insight Fixed potential overflow for the builtin server via the PHP_CLI_SERVER_WORKERS environment variable.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 8.0.22, 8.1.x < 8.1.9 Security Update - Linux OID:1.3.6.1.4.1.25623.1.0.104644 Version used: 2025-01-21T05:37:33Z</p>
<p>Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>References cve: CVE-2022-4900 url: https://www.php.net/ChangeLog-8.php#8.2.0 url: https://www.php.net/ChangeLog-8.php#8.1.9 url: https://www.php.net/ChangeLog-8.php#8.0.22 ... continues on next page ...</p>

...continued from previous page ...
url: https://github.com/php/php-src/issues/8989 url: https://github.com/php/php-src/pull/9000 url: https://github.com/php/php-src/commit/789a37f14405e2d1a05a76c9fb4ed2d49d458 ↪0d5 url: https://bugzilla.redhat.com/show_bug.cgi?id=2179880 cert-bund: WID-SEC-2023-0695 dfn-cert: DFN-CERT-2024-2707 dfn-cert: DFN-CERT-2024-1132 dfn-cert: DFN-CERT-2023-0681

Medium (CVSS: 5.3) NVT: PHP < 7.3.26, 7.4.x < 7.4.14, 8.0.x < 8.0.1 Filter Vulnerability (Jan 2021) - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to a vulnerability where FILTER_VALIDATE_URL accepts URLs with invalid userinfo.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.3.26 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 7.3.26, 7.4.14, 8.0.1 or later.
Affected Software/OS PHP versions prior to 7.3.26, 7.4.x prior to 7.4.14 and 8.0.x prior to 8.0.1.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.3.26, 7.4.x < 7.4.14, 8.0.x < 8.0.1 Filter Vulnerability (Jan 2021) - L. ↪.. OID:1.3.6.1.4.1.25623.1.0.145114 Version used: 2021-11-29T15:00:35Z
Product Detection Result ... continues on next page ...

...continued from previous page ...
Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2020-7071 url: https://www.php.net/ChangeLog-7.php#7.3.26 url: https://www.php.net/ChangeLog-7.php#7.4.14 url: https://www.php.net/ChangeLog-8.php#8.0.1 cert-bund: WID-SEC-2023-1737 cert-bund: WID-SEC-2022-2114 cert-bund: CB-K21/0009 dfn-cert: DFN-CERT-2024-2707 dfn-cert: DFN-CERT-2024-1586 dfn-cert: DFN-CERT-2023-1600 dfn-cert: DFN-CERT-2022-2639 dfn-cert: DFN-CERT-2022-2638 dfn-cert: DFN-CERT-2021-2373 dfn-cert: DFN-CERT-2021-1645 dfn-cert: DFN-CERT-2021-1509 dfn-cert: DFN-CERT-2021-1453 dfn-cert: DFN-CERT-2021-0380 dfn-cert: DFN-CERT-2021-0013

Medium (CVSS: 5.3) NVT: PHP < 7.3.33, 7.4.x < 7.4.26, 8.0.x < 8.0.13 Security Update (Nov 2021) - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP released new versions which include a security fix.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.3.33 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 7.3.33, 7.4.26, 8.0.13 or later.
... continues on next page ...

...continued from previous page ...	
Affected Software/OS PHP prior to version 7.3.33 and version 7.4.x through 7.4.25 and 8.0.x through 8.0.12.	
Vulnerability Insight Fixed bug #79971 (special character is breaking the path in xml function).	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.3.33, 7.4.x < 7.4.26, 8.0.x < 8.0.13 Security Update (Nov 2021) - Linux OID:1.3.6.1.4.1.25623.1.0.147187 Version used: 2021-12-02T03:03:37Z	
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)	
References cve: CVE-2021-21707 url: https://www.php.net/ChangeLog-7.php#7.3.33 url: https://www.php.net/ChangeLog-7.php#7.4.26 url: https://www.php.net/ChangeLog-8.php#8.0.13 url: http://bugs.php.net/79971 cert-bund: WID-SEC-2023-1737 cert-bund: WID-SEC-2022-1767 cert-bund: WID-SEC-2022-0587 cert-bund: WID-SEC-2022-0432 cert-bund: WID-SEC-2022-0302 cert-bund: CB-K21/1213 dfn-cert: DFN-CERT-2023-1600 dfn-cert: DFN-CERT-2022-2869 dfn-cert: DFN-CERT-2022-2639 dfn-cert: DFN-CERT-2022-2638 dfn-cert: DFN-CERT-2022-2598 dfn-cert: DFN-CERT-2022-2499 dfn-cert: DFN-CERT-2022-1516 dfn-cert: DFN-CERT-2022-1493 dfn-cert: DFN-CERT-2022-0557 dfn-cert: DFN-CERT-2022-0485 dfn-cert: DFN-CERT-2022-0455 dfn-cert: DFN-CERT-2022-0431 dfn-cert: DFN-CERT-2022-0407 dfn-cert: DFN-CERT-2022-0110 dfn-cert: DFN-CERT-2021-2474	
... continues on next page ...	

...continued from previous page ...

dfn-cert: DFN-CERT-2021-2436

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://10.0.0.92/mutillidae/src/phpinfo.php>

Concluded from:

```
<title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
↵E" /></head>
```

```
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↵p/7.2/apache2 </td></tr>
```

```
<h2>PHP Variables</h2>
```

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

Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory.

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: phpinfo() Output Reporting (HTTP)

... continues on next page ...

...continued from previous page ...	
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: Enabled Directory Listing/Indexing Detection (HTTP)	
Summary The script attempts to identify directories with an enabled directory listing/indexing on a remote web server.	
Quality of Detection (QoD): 30%	
Vulnerability Detection Result The following directories with an enabled directory listing/indexing were identified: <code>http://10.0.0.92/mutillidae</code> Please review the content manually.	
Impact Based on the information shown an attacker might be able to gather additional info about the structure of this application.	
Solution: Solution type: Mitigation If not needed disable the directory listing/indexing within the web servers config.	
Affected Software/OS Web servers with an enabled directory listing/indexing.	
Vulnerability Detection Method Checks previously detected directories on a remote web server if a directory listing/indexing is enabled. Note: This check has a low QoD (Quality of Detection) value as it is not possible to automatically determine if the directory listing/indexing has been enabled on purpose (which is also a valid use case for some software products). Details: Enabled Directory Listing/Indexing Detection (HTTP) OID:1.3.6.1.4.1.25623.1.0.111074 Version used: 2024-12-17T05:05:41Z	
... continues on next page ...	

...continued from previous page ...	
References cve: CVE-2023-37599 cve: CVE-2024-1076 url: https://wiki.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities_-_Directory_Indexing	
Medium (CVSS: 5.0) NVT: PHP < 7.3.28, 7.4.x < 7.4.18 IMAP Header Injection Vulnerability (Apr 2021) - Linux	
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)	
Summary PHP is prone to an IMAP header injection vulnerability.	
Quality of Detection (QoD): 30%	
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.3.28 Installation path / port: 80/tcp	
Solution: Solution type: VendorFix Update to version 7.3.28, 7.4.18 or later.	
Affected Software/OS PHP versions prior to 7.3.28 and 7.4.x through 7.4.17.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.3.28, 7.4.x < 7.4.18 IMAP Header Injection Vulnerability (Apr 2021) - L. ↪.. OID:1.3.6.1.4.1.25623.1.0.145869 Version used: 2021-05-03T08:21:47Z	
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)	
... continues on next page ...	

...continued from previous page ...

Referencesurl: <https://www.php.net/ChangeLog-7.php#7.3.28>url: <https://www.php.net/ChangeLog-7.php#7.4.18>

Medium (CVSS: 5.0)

NVT: PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Aug 2021) - Linux

Product detection result

cpe:/a:php:php:7.2.34

Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

PHP released new versions which include security fixes.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 7.2.34

Fixed version: 7.3.30

Installation

path / port: 80/tcp

Solution:**Solution type:** VendorFix

Update to version 7.3.30, 7.4.23, 8.0.10 or later.

Affected Software/OS

PHP versions prior to 7.3.30, 7.4.x through 7.4.22 and 8.0.x through 8.0.9.

Vulnerability Detection Method

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

Details: PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Aug 2021) - Linux

OID:1.3.6.1.4.1.25623.1.0.146584

Version used: 2021-08-27T08:15:01Z

Product Detection Result

Product: cpe:/a:php:php:7.2.34

Method: PHP Detection (HTTP)

OID: 1.3.6.1.4.1.25623.1.0.800109)

Referencesurl: <https://www.php.net/ChangeLog-7.php#7.3.30>url: <https://www.php.net/ChangeLog-7.php#7.4.23>url: <https://www.php.net/ChangeLog-8.php#8.0.10>

Medium (CVSS: 5.0)	NVT: Source Control Management (SCM) Files/Folders Accessible (HTTP)
Summary The script attempts to identify files/folders of a SCM accessible at the webserver.	
Quality of Detection (QoD): 70%	
Vulnerability Detection Result The following SCM files/folders were identified: Match: 00000000000000000000000000000000 cede8a534190bb52e7407197e53 ↪d424a7e0cbaf7 root <root@RIS430-Target.(none)> 1741032675 -0500 clone: from ht ↪tps://github.com/digininja/DVWA.git Used regex: ^[a-f0-9]{40} [a-f0-9]{40} URL: http://10.0.0.92/dvwa/.git/logs/HEAD Match: [core] [remote "origin"] [branch "master"] Used regex: ^\[(core receive (remote branch) .+)\] \$ URL: http://10.0.0.92/dvwa/.git/config Match: # git ls-files --others --exclude-from=.git/info/exclude Used regex: ^# git ls-files URL: http://10.0.0.92/dvwa/.git/info/exclude Match: DIRC Used regex: ^DIRC URL: http://10.0.0.92/dvwa/.git/index Match: Unnamed repository; edit this file 'description' to name the repository. ↪ory. Used regex: ^Unnamed repository URL: http://10.0.0.92/dvwa/.git/description Match: ref: refs/heads/master Used regex: ^ref: refs/ URL: http://10.0.0.92/dvwa/.git/HEAD Match: 00000000000000000000000000000000 73d6a092a1cc74580775b2ee510 ↪926fa81d0b46d root <root@RIS430-Target.(none)> 1741032759 -0500 clone: from ht ↪tps://github.com/webpwnized/mutillidae.git Used regex: ^[a-f0-9]{40} [a-f0-9]{40} URL: http://10.0.0.92/mutillidae/.git/logs/HEAD Match: [core] [remote "origin"] [branch "main"] Used regex: ^\[(core receive (remote branch) .+)\] \$ URL: http://10.0.0.92/mutillidae/.git/config Match: # git ls-files --others --exclude-from=.git/info/exclude Used regex: ^# git ls-files URL: http://10.0.0.92/mutillidae/.git/info/exclude ... continues on next page ...	

...continued from previous page...	
Match:	DIRC
Used regex:	^DIRC
URL:	http://10.0.0.92/mutillidae/.git/index
Match:	Unnamed repository; edit this file 'description' to name the repository.
Used regex:	^Unnamed repository
URL:	http://10.0.0.92/mutillidae/.git/description
Match:	ref: refs/heads/main
Used regex:	^ref: refs/
URL:	http://10.0.0.92/mutillidae/.git/HEAD
Impact Based on the information provided in these files/folders an attacker might be able to gather additional info about the structure of the system and its applications.	
Solution: Solution type: Mitigation Restrict access to the SCM files/folders for authorized systems only.	
Vulnerability Insight Currently the script is checking for files/folders of the following SCM software: <ul style="list-style-type: none"> - Git (.git) - Mercurial (.hg) - Bazaar (.bzz) - CVS (CVS/Root, CVS/Entries) - Subversion (.svn) 	
Vulnerability Detection Method Check the response if SCM files/folders are accessible. Details: Source Control Management (SCM) Files/Folders Accessible (HTTP) OID:1.3.6.1.4.1.25623.1.0.111084 Version used: 2023-08-01T13:29:10Z	
References url: http://pen-testing.sans.org/blog/pen-testing/2012/12/06/all-your-svn-are-be-long-to-us url: https://github.com/anantshri/svn-extractor url: https://blog.skullsecurity.org/2012/using-git-clone-to-get-pwn3d url: https://blog.netspi.com/dumping-git-data-from-misconfigured-web-servers/ url: http://resources.infosecinstitute.com/hacking-svn-git-and-mercurial/	
Medium (CVSS: 4.3) NVT: PHP < 8.0.29, 8.1.x < 8.1.20, 8.2.x < 8.2.7 Security Update - Linux	
Product detection result cpe:/a:php:php:7.2.34	
... continues on next page ...	

...continued from previous page ...
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to a missing error check and insufficient random bytes in HTTP Digest authentication for SOAP vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 8.0.29 Installation path / port: 80/tcp
Solution: Solution type: VendorFix Update to version 8.0.29, 8.1.10, 8.2.7 or later.
Affected Software/OS PHP prior to version 8.0.29, 8.1.x prior to 8.1.20 and 8.2.x prior to 8.2.7.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 8.0.29, 8.1.x < 8.1.20, 8.2.x < 8.2.7 Security Update - Linux OID:1.3.6.1.4.1.25623.1.0.149760 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109
References cve: CVE-2023-3247 url: https://www.php.net/ChangeLog-8.php#8.0.29 url: https://www.php.net/ChangeLog-8.php#8.1.20 url: https://www.php.net/ChangeLog-8.php#8.2.7 url: https://github.com/php/php-src/security/advisories/GHSA-76gg-c692-v2mw cert-bund: WID-SEC-2023-2917 cert-bund: WID-SEC-2023-2680 cert-bund: WID-SEC-2023-1506 dfn-cert: DFN-CERT-2024-3330 dfn-cert: DFN-CERT-2023-2570 dfn-cert: DFN-CERT-2023-2542
... continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2023-1328

[\[return to 10.0.0.92 \]](#)

2.2.7 Medium 3128/tcp

Medium (CVSS: 6.5) NVT: Squid DoS Vulnerability (GHSA-j49p-553x-48rx, SQUID-2023:11)
Product detection result cpe:/a:squid-cache:squid:5.9 Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)
Summary Squid is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 5.9 Fixed version: 6.6 Installation path / port: 3128/tcp
Solution: Solution type: VendorFix Update to version 6.6 or later.
Affected Software/OS Squid versions prior to 6.6.
Vulnerability Insight Due to an expired pointer reference bug Squid is vulnerable to a denial of service attack against Cache Manager error responses. This flaw was part of the 'Squid Caching Proxy Security Audit: 55 vulnerabilities and 35 0days' publication in October 2023 and filed as 'Use-After-Free in Cache Manager Errors'.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Squid DoS Vulnerability (GHSA-j49p-553x-48rx, SQUID-2023:11) OID:1.3.6.1.4.1.25623.1.0.151598 Version used: 2024-11-01T05:05:36Z
Product Detection Result ... continues on next page ...

...continued from previous page ...
Product: cpe:/a:squid-cache:squid:5.9 Method: Squid Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.900611)
References cve: CVE-2024-23638 url: https://github.com/squid-cache/squid/security/advisories/GHSA-j49p-553x-48r ↪x url: https://megamansec.github.io/Squid-Security-Audit/ url: https://joshua.hu/squid-security-audit-35-0days-45-exploits url: https://www.openwall.com/lists/oss-security/2023/10/11/3 url: https://gist.github.com/rousskov/9af0d33d2a1f4b5b3b948b2da426e77d url: https://megamansec.github.io/Squid-Security-Audit/cache-uaf.html cert-bund: WID-SEC-2024-0180 dfn-cert: DFN-CERT-2024-3050 dfn-cert: DFN-CERT-2024-1935 dfn-cert: DFN-CERT-2024-1413 dfn-cert: DFN-CERT-2024-1017 dfn-cert: DFN-CERT-2024-0956 dfn-cert: DFN-CERT-2024-0642 dfn-cert: DFN-CERT-2024-0290

Medium (CVSS: 5.3) NVT: Squid Request/Response Smuggling Vulnerability (GHSA-j83v-w3p4-5cqhq, SQUID-2023:1)
Product detection result cpe:/a:squid-cache:squid:5.9 Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)
Summary Squid is prone to a request/response smuggling vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 5.9 Fixed version: 6.4 Installation path / port: 3128/tcp
Solution: Solution type: VendorFix Update to version 6.4 or later.
... continues on next page ...

...continued from previous page ...
Affected Software/OS Squid versions 2.6 through 6.3.
Vulnerability Insight Due to chunked decoder lenience Squid is vulnerable to Request/Response smuggling attacks when parsing HTTP/1.1 and ICAP messages.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Squid Request/Response Smuggling Vulnerability (GHSA-j83v-w3p4-5cqh, SQUID-2023.↔.. OID:1.3.6.1.4.1.25623.1.0.100765 Version used: 2023-11-16T05:05:14Z
Product Detection Result Product: cpe:/a:squid-cache:squid:5.9 Method: Squid Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.900611)
References cve: CVE-2023-46846 url: https://github.com/squid-cache/squid/security/advisories/GHSA-j83v-w3p4-5cqh ↔h cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2023-2725 dfn-cert: DFN-CERT-2024-3343 dfn-cert: DFN-CERT-2024-0642 dfn-cert: DFN-CERT-2024-0039 dfn-cert: DFN-CERT-2023-2934 dfn-cert: DFN-CERT-2023-2781 dfn-cert: DFN-CERT-2023-2746 dfn-cert: DFN-CERT-2023-2712
Medium (CVSS: 4.9) NVT: Squid DoS Vulnerability (GHSA-wgvf-q977-9xjg, SQUID-2024:3)
Product detection result cpe:/a:squid-cache:squid:5.9 Detected by Squid Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900611)
Summary Squid is prone to a denial of service (DoS) vulnerability in ESI processing.
... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 5.9 Fixed version: 6.10 Installation path / port: 3128/tcp
Solution: Solution type: VendorFix Update to version 6.10 or later.
Affected Software/OS Squid version 3.0 through 6.9.
Vulnerability Insight Due to an Out-of-bounds Write error when assigning ESI variables, Squid is susceptible to a Memory Corruption error, which can result in a Denial of Service. This flaw was part of the 'Squid Caching Proxy Security Audit: 55 vulnerabilities and 35 0days' publication in October 2023 and filed as 'Buffer Underflow in ESI'.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Squid DoS Vulnerability (GHSA-wgvf-q977-9xjg, SQUID-2024:3) OID:1.3.6.1.4.1.25623.1.0.114674 Version used: 2024-11-01T05:05:36Z
Product Detection Result Product: cpe:/a:squid-cache:squid:5.9 Method: Squid Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.900611)
References cve: CVE-2024-37894 url: https://github.com/squid-cache/squid/security/advisories/GHSA-wgvf-q977-9xjg ↪g url: https://megamansec.github.io/Squid-Security-Audit/ url: https://joshua.hu/squid-security-audit-35-0days-45-exploits url: https://www.openwall.com/lists/oss-security/2023/10/11/3 url: https://gist.github.com/rousskov/9af0d33d2a1f4b5b3b948b2da426e77d url: https://megamansec.github.io/Squid-Security-Audit/esi-underflow.html cert-bund: WID-SEC-2024-1447 dfn-cert: DFN-CERT-2024-1935 dfn-cert: DFN-CERT-2024-1706

[\[return to 10.0.0.92 \]](#)

2.2.8 Medium 21/tcp

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

[\[return to 10.0.0.92 \]](#)

2.2.9 Medium general/tcp

Medium (CVSS: 6.5) NVT: Samba Multiple Vulnerabilities (Mar 2023)
Product detection result cpe:/a:samba:samba:4.15.13 Detected by Samba Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800403)
... continues on next page ...

...continued from previous page ...
Summary Samba is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 4.15.13 Fixed version: 4.16.10 / 4.17.7 / 4.18.1 Installation path / port: /usr/sbin/smbd
Solution: Solution type: VendorFix Update to version 4.16.10, 4.17.7, 4.18.1 or later.
Affected Software/OS All versions of Samba since 4.0.
Vulnerability Insight The following flaws exist: - CVE-2023-0614: Access controlled AD LDAP attributes can be discovered - CVE-2023-0922: Samba AD DC admin tool samba-tool sends passwords in cleartext
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Samba Multiple Vulnerabilities (Mar 2023) OID: 1.3.6.1.4.1.25623.1.0.104663 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:samba:samba:4.15.13 Method: Samba Version Detection OID: 1.3.6.1.4.1.25623.1.0.800403)
References cve: CVE-2023-0614 cve: CVE-2023-0922 url: https://www.samba.org/samba/security/CVE-2023-0614.html url: https://www.samba.org/samba/security/CVE-2023-0922.html cert-bund: WID-SEC-2023-0796 dfn-cert: DFN-CERT-2023-0858 dfn-cert: DFN-CERT-2023-0857 dfn-cert: DFN-CERT-2023-0713
... continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2023-0710
 dfn-cert: DFN-CERT-2023-0707

Medium (CVSS: 6.5)

NVT: Samba File Truncation Vulnerability (CVE-2023-3347)

Product detection result

cpe:/a:samba:samba:4.15.13

Detected by Samba Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800403)

Summary

Samba is prone to a file truncation vulnerability.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 4.15.13

Fixed version: 4.17.12 / 4.18.8 / 4.19.1

Installation

path / port: /usr/sbin/smbd

Solution:**Solution type:** VendorFix

Update to version 4.17.12, 4.18.8, 4.19.1 or later.

Affected Software/OS

Samba versions prior to 4.17.12, 4.18.x prior to 4.18.8 and 4.19.0 only.

Vulnerability Insight

SMB client can truncate files to 0 bytes by opening files with OVERWRITE disposition when using the acl_xattr Samba VFS module with the smb.conf setting 'acl_xattr:ignore system acls = yes'.

Vulnerability Detection Method

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

Details: Samba File Truncation Vulnerability (CVE-2023-3347)

OID:1.3.6.1.4.1.25623.1.0.104957

Version used: 2023-11-16T05:05:14Z

Product Detection Result

Product: cpe:/a:samba:samba:4.15.13

Method: Samba Version Detection

OID: 1.3.6.1.4.1.25623.1.0.800403)

... continues on next page ...

...continued from previous page ...

References

cve: CVE-2023-4091
 url: <https://lists.samba.org/archive/samba-announce/2023/000651.html>
 url: <https://www.samba.org/samba/security/CVE-2023-4091.html>
 cert-bund: WID-SEC-2023-2620
 dfn-cert: DFN-CERT-2024-1065
 dfn-cert: DFN-CERT-2024-0839
 dfn-cert: DFN-CERT-2023-2700
 dfn-cert: DFN-CERT-2023-2494
 dfn-cert: DFN-CERT-2023-2462
 dfn-cert: DFN-CERT-2023-2447
 dfn-cert: DFN-CERT-2023-2443

Medium (CVSS: 6.5)

NVT: Samba 4.0.0 < 4.17.12, 4.18.0 < 4.18.8, 4.19.0 Multiple Vulnerabilities

Product detection result

cpe:/a:samba:samba:4.15.13
 Detected by Samba Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800403)

Summary

Samba is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 4.15.13
 Fixed version: 4.17.12 / 4.18.8 / 4.19.1
 Installation
 path / port: /usr/sbin/smbd

Solution:

Solution type: VendorFix
 Update to version 4.17.12, 4.18.8, 4.19.1 or later.

Affected Software/OS

All versions of Samba since 4.0.0.

Vulnerability Insight

The following flaws exist:
 - CVE-2023-4154: Samba AD DC password exposure to privileged users and RODCs
 - CVE-2023-42669: 'rpcecho' development server allows Denial of Service via sleep() call on AD DC

... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Samba 4.0.0 < 4.17.12, 4.18.0 < 4.18.8, 4.19.0 Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.104958 Version used: 2023-11-16T05:05:14Z
Product Detection Result Product: cpe:/a:samba:samba:4.15.13 Method: Samba Version Detection OID: 1.3.6.1.4.1.25623.1.0.800403)
References cve: CVE-2023-4154 cve: CVE-2023-42669 url: https://lists.samba.org/archive/samba-announce/2023/000651.html url: https://www.samba.org/samba/security/CVE-2023-4154.html url: https://www.samba.org/samba/security/CVE-2023-42669.html cert-bund: WID-SEC-2024-0523 cert-bund: WID-SEC-2023-2620 dfn-cert: DFN-CERT-2023-2700 dfn-cert: DFN-CERT-2023-2494 dfn-cert: DFN-CERT-2023-2447 dfn-cert: DFN-CERT-2023-2443

Medium (CVSS: 6.5) NVT: PHP < 7.3.31, 7.4.x < 7.4.24, 8.0.x < 8.0.11 Security Update (Sep 2021) - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP released new versions which includes a security fix.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.3.31 Installation path / port: /usr/bin/php7.2
Solution: Solution type: VendorFix
... continues on next page ...

...continued from previous page ...
Update to version 7.3.31, 7.4.24, 8.0.11 or later.
Affected Software/OS PHP versions prior to 7.3.31, 7.4.x through 7.4.23 and 8.0.x through 8.0.10.
Vulnerability Insight Fixed bug #81420 (ZipArchive::extractTo extracts outside of destination).
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.3.31, 7.4.x < 7.4.24, 8.0.x < 8.0.11 Security Update (Sep 2021) - Linux OID: 1.3.6.1.4.1.25623.1.0.117694 Version used: 2021-10-11T08:01:31Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109
References cve: CVE-2021-21706 url: https://www.php.net/ChangeLog-7.php#7.3.31 url: https://www.php.net/ChangeLog-7.php#7.4.24 url: https://www.php.net/ChangeLog-8.php#8.0.11 url: http://bugs.php.net/81420 cert-bund: WID-SEC-2022-2112 cert-bund: CB-K21/1008 dfn-cert: DFN-CERT-2022-2639 dfn-cert: DFN-CERT-2021-2474 dfn-cert: DFN-CERT-2021-1994
Medium (CVSS: 6.5) NVT: OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities (Terrapin Attack)
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.6 Installation path / port: /usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.6 or later. Note: Client and Server implementations need to run a fixed version to mitigate the Terrapin flaw.
Affected Software/OS OpenBSD OpenSSH prior to version 9.6.
Vulnerability Insight The following vulnerabilities exist: - CVE-2023-48795: The SSH transport protocol with certain OpenSSH extensions allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a 'Terrapin attack'. - CVE-2023-51384: In ssh-agent certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys. - CVE-2023-51385: OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities (Terrapin Attack) OID:1.3.6.1.4.1.25623.1.0.118572 Version used: 2024-03-15T05:06:15Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2023-48795 cve: CVE-2023-51384 cve: CVE-2023-51385
... continues on next page ...

...continued from previous page ...

```
url: https://www.openssh.com/txt/release-9.6
url: https://terrapin-attack.com
url: https://vin01.github.io/piptagole/ssh/security/openssh/libssh/remote-code-e
↪xecution/2023/12/20/openssh-proxycommand-libssh-rce.html
cert-bund: WID-SEC-2025-0168
cert-bund: WID-SEC-2025-0144
cert-bund: WID-SEC-2025-0139
cert-bund: WID-SEC-2024-3377
cert-bund: WID-SEC-2024-3320
cert-bund: WID-SEC-2024-3198
cert-bund: WID-SEC-2024-3195
cert-bund: WID-SEC-2024-3140
cert-bund: WID-SEC-2024-1913
cert-bund: WID-SEC-2024-1781
cert-bund: WID-SEC-2024-1701
cert-bund: WID-SEC-2024-1656
cert-bund: WID-SEC-2024-1655
cert-bund: WID-SEC-2024-1643
cert-bund: WID-SEC-2024-1642
cert-bund: WID-SEC-2024-1639
cert-bund: WID-SEC-2024-1637
cert-bund: WID-SEC-2024-1630
cert-bund: WID-SEC-2024-1474
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-1228
cert-bund: WID-SEC-2024-1186
cert-bund: WID-SEC-2024-1082
cert-bund: WID-SEC-2024-0899
cert-bund: WID-SEC-2024-0892
cert-bund: WID-SEC-2024-0889
cert-bund: WID-SEC-2024-0885
cert-bund: WID-SEC-2024-0874
cert-bund: WID-SEC-2024-0869
cert-bund: WID-SEC-2024-0578
cert-bund: WID-SEC-2024-0564
cert-bund: WID-SEC-2024-0523
cert-bund: WID-SEC-2023-3182
cert-bund: WID-SEC-2023-3174
dfn-cert: DFN-CERT-2025-0294
dfn-cert: DFN-CERT-2025-0173
dfn-cert: DFN-CERT-2025-0165
dfn-cert: DFN-CERT-2025-0024
dfn-cert: DFN-CERT-2024-3171
dfn-cert: DFN-CERT-2024-2818
dfn-cert: DFN-CERT-2024-2759
dfn-cert: DFN-CERT-2024-2741
dfn-cert: DFN-CERT-2024-2682
```

...continues on next page ...

...continued from previous page ...

```

dfn-cert: DFN-CERT-2024-2602
dfn-cert: DFN-CERT-2024-2573
dfn-cert: DFN-CERT-2024-2392
dfn-cert: DFN-CERT-2024-2210
dfn-cert: DFN-CERT-2024-2209
dfn-cert: DFN-CERT-2024-2194
dfn-cert: DFN-CERT-2024-2169
dfn-cert: DFN-CERT-2024-2048
dfn-cert: DFN-CERT-2024-2030
dfn-cert: DFN-CERT-2024-2028
dfn-cert: DFN-CERT-2024-1930
dfn-cert: DFN-CERT-2024-1895
dfn-cert: DFN-CERT-2024-1869
dfn-cert: DFN-CERT-2024-1868
dfn-cert: DFN-CERT-2024-1865
dfn-cert: DFN-CERT-2024-1862
dfn-cert: DFN-CERT-2024-1854
dfn-cert: DFN-CERT-2024-1846
dfn-cert: DFN-CERT-2024-1817
dfn-cert: DFN-CERT-2024-1794
dfn-cert: DFN-CERT-2024-1715
dfn-cert: DFN-CERT-2024-1698
dfn-cert: DFN-CERT-2024-1688
dfn-cert: DFN-CERT-2024-1655
dfn-cert: DFN-CERT-2024-1600
dfn-cert: DFN-CERT-2024-1443
dfn-cert: DFN-CERT-2024-1442
dfn-cert: DFN-CERT-2024-1413
dfn-cert: DFN-CERT-2024-1382
dfn-cert: DFN-CERT-2024-1380
dfn-cert: DFN-CERT-2024-1373
dfn-cert: DFN-CERT-2024-1260
dfn-cert: DFN-CERT-2024-1259
dfn-cert: DFN-CERT-2024-1108
dfn-cert: DFN-CERT-2024-1061
dfn-cert: DFN-CERT-2024-1029
dfn-cert: DFN-CERT-2024-1003
dfn-cert: DFN-CERT-2024-1000
dfn-cert: DFN-CERT-2024-0896
dfn-cert: DFN-CERT-2024-0779
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0744
dfn-cert: DFN-CERT-2024-0698
dfn-cert: DFN-CERT-2024-0633
dfn-cert: DFN-CERT-2024-0619
dfn-cert: DFN-CERT-2024-0618
dfn-cert: DFN-CERT-2024-0616

```

...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2024-0597
dfn-cert: DFN-CERT-2024-0545
dfn-cert: DFN-CERT-2024-0526
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0480
dfn-cert: DFN-CERT-2024-0451
dfn-cert: DFN-CERT-2024-0440
dfn-cert: DFN-CERT-2024-0420
dfn-cert: DFN-CERT-2024-0388
dfn-cert: DFN-CERT-2024-0343
dfn-cert: DFN-CERT-2024-0306
dfn-cert: DFN-CERT-2024-0299
dfn-cert: DFN-CERT-2024-0285
dfn-cert: DFN-CERT-2024-0267
dfn-cert: DFN-CERT-2024-0251
dfn-cert: DFN-CERT-2024-0215
dfn-cert: DFN-CERT-2024-0211
dfn-cert: DFN-CERT-2024-0164
dfn-cert: DFN-CERT-2024-0154
dfn-cert: DFN-CERT-2024-0101
dfn-cert: DFN-CERT-2024-0092
dfn-cert: DFN-CERT-2024-0088
dfn-cert: DFN-CERT-2024-0067
dfn-cert: DFN-CERT-2024-0063
dfn-cert: DFN-CERT-2024-0062
dfn-cert: DFN-CERT-2024-0024
dfn-cert: DFN-CERT-2024-0022
dfn-cert: DFN-CERT-2024-0013
dfn-cert: DFN-CERT-2023-3219
dfn-cert: DFN-CERT-2023-3218
dfn-cert: DFN-CERT-2023-3210
dfn-cert: DFN-CERT-2023-3201
dfn-cert: DFN-CERT-2023-3200
dfn-cert: DFN-CERT-2023-3195
dfn-cert: DFN-CERT-2023-3193
dfn-cert: DFN-CERT-2023-3191
dfn-cert: DFN-CERT-2023-3185
dfn-cert: DFN-CERT-2023-3184
dfn-cert: DFN-CERT-2023-3183
dfn-cert: DFN-CERT-2023-3182
dfn-cert: DFN-CERT-2023-3175

Medium (CVSS: 6.5)

NVT: OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities (Terrapin Attack)

Product detection result

cpe:/a:openbsd:openssh:8.9p1

... continues on next page ...

...continued from previous page ...
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.6 Installation path / port: /usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.6 or later. Note: Client and Server implementations need to run a fixed version to mitigate the Terrapin flaw.
Affected Software/OS OpenBSD OpenSSH prior to version 9.6.
Vulnerability Insight The following vulnerabilities exist: - CVE-2023-48795: The SSH transport protocol with certain OpenSSH extensions allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a 'Terrapin attack'. - CVE-2023-51384: In ssh-agent certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys. - CVE-2023-51385: OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities (Terrapin Attack) OID:1.3.6.1.4.1.25623.1.0.118572 Version used: 2024-03-15T05:06:15Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1
... continues on next page ...

...continued from previous page ...
Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2023-48795 cve: CVE-2023-51384 cve: CVE-2023-51385 url: https://www.openssh.com/txt/release-9.6 url: https://terrapin-attack.com url: https://vin01.github.io/piptagole/ssh/security/openssh/libssh/remote-code-e↵xecution/2023/12/20/openssh-proxycommand-libssh-rce.html cert-bund: WID-SEC-2025-0168 cert-bund: WID-SEC-2025-0144 cert-bund: WID-SEC-2025-0139 cert-bund: WID-SEC-2024-3377 cert-bund: WID-SEC-2024-3320 cert-bund: WID-SEC-2024-3198 cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-3140 cert-bund: WID-SEC-2024-1913 cert-bund: WID-SEC-2024-1781 cert-bund: WID-SEC-2024-1701 cert-bund: WID-SEC-2024-1656 cert-bund: WID-SEC-2024-1655 cert-bund: WID-SEC-2024-1643 cert-bund: WID-SEC-2024-1642 cert-bund: WID-SEC-2024-1639 cert-bund: WID-SEC-2024-1637 cert-bund: WID-SEC-2024-1630 cert-bund: WID-SEC-2024-1474 cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2024-1228 cert-bund: WID-SEC-2024-1186 cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2024-0899 cert-bund: WID-SEC-2024-0892 cert-bund: WID-SEC-2024-0889 cert-bund: WID-SEC-2024-0885 cert-bund: WID-SEC-2024-0874 cert-bund: WID-SEC-2024-0869 cert-bund: WID-SEC-2024-0578 cert-bund: WID-SEC-2024-0564 cert-bund: WID-SEC-2024-0523 cert-bund: WID-SEC-2023-3182 cert-bund: WID-SEC-2023-3174 dfn-cert: DFN-CERT-2025-0294
... continues on next page ...

...continued from previous page ...

```

dfn-cert: DFN-CERT-2025-0173
dfn-cert: DFN-CERT-2025-0165
dfn-cert: DFN-CERT-2025-0024
dfn-cert: DFN-CERT-2024-3171
dfn-cert: DFN-CERT-2024-2818
dfn-cert: DFN-CERT-2024-2759
dfn-cert: DFN-CERT-2024-2741
dfn-cert: DFN-CERT-2024-2682
dfn-cert: DFN-CERT-2024-2602
dfn-cert: DFN-CERT-2024-2573
dfn-cert: DFN-CERT-2024-2392
dfn-cert: DFN-CERT-2024-2210
dfn-cert: DFN-CERT-2024-2209
dfn-cert: DFN-CERT-2024-2194
dfn-cert: DFN-CERT-2024-2169
dfn-cert: DFN-CERT-2024-2048
dfn-cert: DFN-CERT-2024-2030
dfn-cert: DFN-CERT-2024-2028
dfn-cert: DFN-CERT-2024-1930
dfn-cert: DFN-CERT-2024-1895
dfn-cert: DFN-CERT-2024-1869
dfn-cert: DFN-CERT-2024-1868
dfn-cert: DFN-CERT-2024-1865
dfn-cert: DFN-CERT-2024-1862
dfn-cert: DFN-CERT-2024-1854
dfn-cert: DFN-CERT-2024-1846
dfn-cert: DFN-CERT-2024-1817
dfn-cert: DFN-CERT-2024-1794
dfn-cert: DFN-CERT-2024-1715
dfn-cert: DFN-CERT-2024-1698
dfn-cert: DFN-CERT-2024-1688
dfn-cert: DFN-CERT-2024-1655
dfn-cert: DFN-CERT-2024-1600
dfn-cert: DFN-CERT-2024-1443
dfn-cert: DFN-CERT-2024-1442
dfn-cert: DFN-CERT-2024-1413
dfn-cert: DFN-CERT-2024-1382
dfn-cert: DFN-CERT-2024-1380
dfn-cert: DFN-CERT-2024-1373
dfn-cert: DFN-CERT-2024-1260
dfn-cert: DFN-CERT-2024-1259
dfn-cert: DFN-CERT-2024-1108
dfn-cert: DFN-CERT-2024-1061
dfn-cert: DFN-CERT-2024-1029
dfn-cert: DFN-CERT-2024-1003
dfn-cert: DFN-CERT-2024-1000
dfn-cert: DFN-CERT-2024-0896

```

...continues on next page ...

...continued from previous page ...

```

dfn-cert: DFN-CERT-2024-0779
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0744
dfn-cert: DFN-CERT-2024-0698
dfn-cert: DFN-CERT-2024-0633
dfn-cert: DFN-CERT-2024-0619
dfn-cert: DFN-CERT-2024-0618
dfn-cert: DFN-CERT-2024-0616
dfn-cert: DFN-CERT-2024-0597
dfn-cert: DFN-CERT-2024-0545
dfn-cert: DFN-CERT-2024-0526
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0480
dfn-cert: DFN-CERT-2024-0451
dfn-cert: DFN-CERT-2024-0440
dfn-cert: DFN-CERT-2024-0420
dfn-cert: DFN-CERT-2024-0388
dfn-cert: DFN-CERT-2024-0343
dfn-cert: DFN-CERT-2024-0306
dfn-cert: DFN-CERT-2024-0299
dfn-cert: DFN-CERT-2024-0285
dfn-cert: DFN-CERT-2024-0267
dfn-cert: DFN-CERT-2024-0251
dfn-cert: DFN-CERT-2024-0215
dfn-cert: DFN-CERT-2024-0211
dfn-cert: DFN-CERT-2024-0164
dfn-cert: DFN-CERT-2024-0154
dfn-cert: DFN-CERT-2024-0101
dfn-cert: DFN-CERT-2024-0092
dfn-cert: DFN-CERT-2024-0088
dfn-cert: DFN-CERT-2024-0067
dfn-cert: DFN-CERT-2024-0063
dfn-cert: DFN-CERT-2024-0062
dfn-cert: DFN-CERT-2024-0024
dfn-cert: DFN-CERT-2024-0022
dfn-cert: DFN-CERT-2024-0013
dfn-cert: DFN-CERT-2023-3219
dfn-cert: DFN-CERT-2023-3218
dfn-cert: DFN-CERT-2023-3210
dfn-cert: DFN-CERT-2023-3201
dfn-cert: DFN-CERT-2023-3200
dfn-cert: DFN-CERT-2023-3195
dfn-cert: DFN-CERT-2023-3193
dfn-cert: DFN-CERT-2023-3191
dfn-cert: DFN-CERT-2023-3185
dfn-cert: DFN-CERT-2023-3184
dfn-cert: DFN-CERT-2023-3183

```

...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2023-3182 dfn-cert: DFN-CERT-2023-3175
Medium (CVSS: 6.5) NVT: OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities (Terrapin Attack)
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.6 Installation path / port: /snap/core22/1748/usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.6 or later. Note: Client and Server implementations need to run a fixed version to mitigate the Terrapin flaw.
Affected Software/OS OpenBSD OpenSSH prior to version 9.6.
Vulnerability Insight The following vulnerabilities exist: - CVE-2023-48795: The SSH transport protocol with certain OpenSSH extensions allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a 'Terrapin attack'. - CVE-2023-51384: In ssh-agent certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys. - CVE-2023-51385: OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.
... continues on next page ...

...continued from previous page ...

Vulnerability Detection Method

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

Details: OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities (Terrapin Attack)

OID:1.3.6.1.4.1.25623.1.0.118572

Version used: 2024-03-15T05:06:15Z

Product Detection Result

Product: cpe:/a:openbsd:openssh:8.9p1

Method: OpenSSH Detection Consolidation

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

cve: CVE-2023-48795

cve: CVE-2023-51384

cve: CVE-2023-51385

url: <https://www.openssh.com/txt/release-9.6>url: <https://terrapin-attack.com>url: <https://vin01.github.io/piptagole/ssh/security/openssh/libssh/remote-code-e↵xecution/2023/12/20/openssh-proxycommand-libssh-rce.html>

cert-bund: WID-SEC-2025-0168

cert-bund: WID-SEC-2025-0144

cert-bund: WID-SEC-2025-0139

cert-bund: WID-SEC-2024-3377

cert-bund: WID-SEC-2024-3320

cert-bund: WID-SEC-2024-3198

cert-bund: WID-SEC-2024-3195

cert-bund: WID-SEC-2024-3140

cert-bund: WID-SEC-2024-1913

cert-bund: WID-SEC-2024-1781

cert-bund: WID-SEC-2024-1701

cert-bund: WID-SEC-2024-1656

cert-bund: WID-SEC-2024-1655

cert-bund: WID-SEC-2024-1643

cert-bund: WID-SEC-2024-1642

cert-bund: WID-SEC-2024-1639

cert-bund: WID-SEC-2024-1637

cert-bund: WID-SEC-2024-1630

cert-bund: WID-SEC-2024-1474

cert-bund: WID-SEC-2024-1248

cert-bund: WID-SEC-2024-1228

cert-bund: WID-SEC-2024-1186

cert-bund: WID-SEC-2024-1082

cert-bund: WID-SEC-2024-0899

cert-bund: WID-SEC-2024-0892

cert-bund: WID-SEC-2024-0889

... continues on next page ...

...continued from previous page ...

cert-bund: WID-SEC-2024-0885
 cert-bund: WID-SEC-2024-0874
 cert-bund: WID-SEC-2024-0869
 cert-bund: WID-SEC-2024-0578
 cert-bund: WID-SEC-2024-0564
 cert-bund: WID-SEC-2024-0523
 cert-bund: WID-SEC-2023-3182
 cert-bund: WID-SEC-2023-3174
 dfn-cert: DFN-CERT-2025-0294
 dfn-cert: DFN-CERT-2025-0173
 dfn-cert: DFN-CERT-2025-0165
 dfn-cert: DFN-CERT-2025-0024
 dfn-cert: DFN-CERT-2024-3171
 dfn-cert: DFN-CERT-2024-2818
 dfn-cert: DFN-CERT-2024-2759
 dfn-cert: DFN-CERT-2024-2741
 dfn-cert: DFN-CERT-2024-2682
 dfn-cert: DFN-CERT-2024-2602
 dfn-cert: DFN-CERT-2024-2573
 dfn-cert: DFN-CERT-2024-2392
 dfn-cert: DFN-CERT-2024-2210
 dfn-cert: DFN-CERT-2024-2209
 dfn-cert: DFN-CERT-2024-2194
 dfn-cert: DFN-CERT-2024-2169
 dfn-cert: DFN-CERT-2024-2048
 dfn-cert: DFN-CERT-2024-2030
 dfn-cert: DFN-CERT-2024-2028
 dfn-cert: DFN-CERT-2024-1930
 dfn-cert: DFN-CERT-2024-1895
 dfn-cert: DFN-CERT-2024-1869
 dfn-cert: DFN-CERT-2024-1868
 dfn-cert: DFN-CERT-2024-1865
 dfn-cert: DFN-CERT-2024-1862
 dfn-cert: DFN-CERT-2024-1854
 dfn-cert: DFN-CERT-2024-1846
 dfn-cert: DFN-CERT-2024-1817
 dfn-cert: DFN-CERT-2024-1794
 dfn-cert: DFN-CERT-2024-1715
 dfn-cert: DFN-CERT-2024-1698
 dfn-cert: DFN-CERT-2024-1688
 dfn-cert: DFN-CERT-2024-1655
 dfn-cert: DFN-CERT-2024-1600
 dfn-cert: DFN-CERT-2024-1443
 dfn-cert: DFN-CERT-2024-1442
 dfn-cert: DFN-CERT-2024-1413
 dfn-cert: DFN-CERT-2024-1382
 dfn-cert: DFN-CERT-2024-1380

...continues on next page ...

...continued from previous page ...

```

dfn-cert: DFN-CERT-2024-1373
dfn-cert: DFN-CERT-2024-1260
dfn-cert: DFN-CERT-2024-1259
dfn-cert: DFN-CERT-2024-1108
dfn-cert: DFN-CERT-2024-1061
dfn-cert: DFN-CERT-2024-1029
dfn-cert: DFN-CERT-2024-1003
dfn-cert: DFN-CERT-2024-1000
dfn-cert: DFN-CERT-2024-0896
dfn-cert: DFN-CERT-2024-0779
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0744
dfn-cert: DFN-CERT-2024-0698
dfn-cert: DFN-CERT-2024-0633
dfn-cert: DFN-CERT-2024-0619
dfn-cert: DFN-CERT-2024-0618
dfn-cert: DFN-CERT-2024-0616
dfn-cert: DFN-CERT-2024-0597
dfn-cert: DFN-CERT-2024-0545
dfn-cert: DFN-CERT-2024-0526
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0480
dfn-cert: DFN-CERT-2024-0451
dfn-cert: DFN-CERT-2024-0440
dfn-cert: DFN-CERT-2024-0420
dfn-cert: DFN-CERT-2024-0388
dfn-cert: DFN-CERT-2024-0343
dfn-cert: DFN-CERT-2024-0306
dfn-cert: DFN-CERT-2024-0299
dfn-cert: DFN-CERT-2024-0285
dfn-cert: DFN-CERT-2024-0267
dfn-cert: DFN-CERT-2024-0251
dfn-cert: DFN-CERT-2024-0215
dfn-cert: DFN-CERT-2024-0211
dfn-cert: DFN-CERT-2024-0164
dfn-cert: DFN-CERT-2024-0154
dfn-cert: DFN-CERT-2024-0101
dfn-cert: DFN-CERT-2024-0092
dfn-cert: DFN-CERT-2024-0088
dfn-cert: DFN-CERT-2024-0067
dfn-cert: DFN-CERT-2024-0063
dfn-cert: DFN-CERT-2024-0062
dfn-cert: DFN-CERT-2024-0024
dfn-cert: DFN-CERT-2024-0022
dfn-cert: DFN-CERT-2024-0013
dfn-cert: DFN-CERT-2023-3219
dfn-cert: DFN-CERT-2023-3218

```

...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2023-3210 dfn-cert: DFN-CERT-2023-3201 dfn-cert: DFN-CERT-2023-3200 dfn-cert: DFN-CERT-2023-3195 dfn-cert: DFN-CERT-2023-3193 dfn-cert: DFN-CERT-2023-3191 dfn-cert: DFN-CERT-2023-3185 dfn-cert: DFN-CERT-2023-3184 dfn-cert: DFN-CERT-2023-3183 dfn-cert: DFN-CERT-2023-3182 dfn-cert: DFN-CERT-2023-3175
Medium (CVSS: 6.5) NVT: OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities (Terrapin Attack)
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.6 Installation path / port: /snap/core22/1748/usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.6 or later. Note: Client and Server implementations need to run a fixed version to mitigate the Terrapin flaw.
Affected Software/OS OpenBSD OpenSSH prior to version 9.6.
Vulnerability Insight The following vulnerabilities exist: - CVE-2023-48795: The SSH transport protocol with certain OpenSSH extensions allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a 'Terrapin attack'.
... continues on next page ...

...continued from previous page ...
<p>- CVE-2023-51384: In ssh-agent certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys.</p> <p>- CVE-2023-51385: OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities (Terrapin Attack) OID:1.3.6.1.4.1.25623.1.0.118572 Version used: 2024-03-15T05:06:15Z</p>
<p>Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>References cve: CVE-2023-48795 cve: CVE-2023-51384 cve: CVE-2023-51385 url: https://www.openssh.com/txt/release-9.6 url: https://terrapin-attack.com url: https://vin01.github.io/piptagole/ssh/security/openssh/libssh/remote-code-e ↪xecution/2023/12/20/openssh-proxycommand-libssh-rce.html cert-bund: WID-SEC-2025-0168 cert-bund: WID-SEC-2025-0144 cert-bund: WID-SEC-2025-0139 cert-bund: WID-SEC-2024-3377 cert-bund: WID-SEC-2024-3320 cert-bund: WID-SEC-2024-3198 cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-3140 cert-bund: WID-SEC-2024-1913 cert-bund: WID-SEC-2024-1781 cert-bund: WID-SEC-2024-1701 cert-bund: WID-SEC-2024-1656 cert-bund: WID-SEC-2024-1655 cert-bund: WID-SEC-2024-1643 cert-bund: WID-SEC-2024-1642 cert-bund: WID-SEC-2024-1639 cert-bund: WID-SEC-2024-1637 cert-bund: WID-SEC-2024-1630</p>
...continues on next page ...

...continued from previous page ...	
cert-bund:	WID-SEC-2024-1474
cert-bund:	WID-SEC-2024-1248
cert-bund:	WID-SEC-2024-1228
cert-bund:	WID-SEC-2024-1186
cert-bund:	WID-SEC-2024-1082
cert-bund:	WID-SEC-2024-0899
cert-bund:	WID-SEC-2024-0892
cert-bund:	WID-SEC-2024-0889
cert-bund:	WID-SEC-2024-0885
cert-bund:	WID-SEC-2024-0874
cert-bund:	WID-SEC-2024-0869
cert-bund:	WID-SEC-2024-0578
cert-bund:	WID-SEC-2024-0564
cert-bund:	WID-SEC-2024-0523
cert-bund:	WID-SEC-2023-3182
cert-bund:	WID-SEC-2023-3174
dfn-cert:	DFN-CERT-2025-0294
dfn-cert:	DFN-CERT-2025-0173
dfn-cert:	DFN-CERT-2025-0165
dfn-cert:	DFN-CERT-2025-0024
dfn-cert:	DFN-CERT-2024-3171
dfn-cert:	DFN-CERT-2024-2818
dfn-cert:	DFN-CERT-2024-2759
dfn-cert:	DFN-CERT-2024-2741
dfn-cert:	DFN-CERT-2024-2682
dfn-cert:	DFN-CERT-2024-2602
dfn-cert:	DFN-CERT-2024-2573
dfn-cert:	DFN-CERT-2024-2392
dfn-cert:	DFN-CERT-2024-2210
dfn-cert:	DFN-CERT-2024-2209
dfn-cert:	DFN-CERT-2024-2194
dfn-cert:	DFN-CERT-2024-2169
dfn-cert:	DFN-CERT-2024-2048
dfn-cert:	DFN-CERT-2024-2030
dfn-cert:	DFN-CERT-2024-2028
dfn-cert:	DFN-CERT-2024-1930
dfn-cert:	DFN-CERT-2024-1895
dfn-cert:	DFN-CERT-2024-1869
dfn-cert:	DFN-CERT-2024-1868
dfn-cert:	DFN-CERT-2024-1865
dfn-cert:	DFN-CERT-2024-1862
dfn-cert:	DFN-CERT-2024-1854
dfn-cert:	DFN-CERT-2024-1846
dfn-cert:	DFN-CERT-2024-1817
dfn-cert:	DFN-CERT-2024-1794
dfn-cert:	DFN-CERT-2024-1715
dfn-cert:	DFN-CERT-2024-1698
...continues on next page ...	

...continued from previous page ...

```

dfn-cert: DFN-CERT-2024-1688
dfn-cert: DFN-CERT-2024-1655
dfn-cert: DFN-CERT-2024-1600
dfn-cert: DFN-CERT-2024-1443
dfn-cert: DFN-CERT-2024-1442
dfn-cert: DFN-CERT-2024-1413
dfn-cert: DFN-CERT-2024-1382
dfn-cert: DFN-CERT-2024-1380
dfn-cert: DFN-CERT-2024-1373
dfn-cert: DFN-CERT-2024-1260
dfn-cert: DFN-CERT-2024-1259
dfn-cert: DFN-CERT-2024-1108
dfn-cert: DFN-CERT-2024-1061
dfn-cert: DFN-CERT-2024-1029
dfn-cert: DFN-CERT-2024-1003
dfn-cert: DFN-CERT-2024-1000
dfn-cert: DFN-CERT-2024-0896
dfn-cert: DFN-CERT-2024-0779
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0744
dfn-cert: DFN-CERT-2024-0698
dfn-cert: DFN-CERT-2024-0633
dfn-cert: DFN-CERT-2024-0619
dfn-cert: DFN-CERT-2024-0618
dfn-cert: DFN-CERT-2024-0616
dfn-cert: DFN-CERT-2024-0597
dfn-cert: DFN-CERT-2024-0545
dfn-cert: DFN-CERT-2024-0526
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0480
dfn-cert: DFN-CERT-2024-0451
dfn-cert: DFN-CERT-2024-0440
dfn-cert: DFN-CERT-2024-0420
dfn-cert: DFN-CERT-2024-0388
dfn-cert: DFN-CERT-2024-0343
dfn-cert: DFN-CERT-2024-0306
dfn-cert: DFN-CERT-2024-0299
dfn-cert: DFN-CERT-2024-0285
dfn-cert: DFN-CERT-2024-0267
dfn-cert: DFN-CERT-2024-0251
dfn-cert: DFN-CERT-2024-0215
dfn-cert: DFN-CERT-2024-0211
dfn-cert: DFN-CERT-2024-0164
dfn-cert: DFN-CERT-2024-0154
dfn-cert: DFN-CERT-2024-0101
dfn-cert: DFN-CERT-2024-0092
dfn-cert: DFN-CERT-2024-0088

```

...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2024-0067
dfn-cert: DFN-CERT-2024-0063
dfn-cert: DFN-CERT-2024-0062
dfn-cert: DFN-CERT-2024-0024
dfn-cert: DFN-CERT-2024-0022
dfn-cert: DFN-CERT-2024-0013
dfn-cert: DFN-CERT-2023-3219
dfn-cert: DFN-CERT-2023-3218
dfn-cert: DFN-CERT-2023-3210
dfn-cert: DFN-CERT-2023-3201
dfn-cert: DFN-CERT-2023-3200
dfn-cert: DFN-CERT-2023-3195
dfn-cert: DFN-CERT-2023-3193
dfn-cert: DFN-CERT-2023-3191
dfn-cert: DFN-CERT-2023-3185
dfn-cert: DFN-CERT-2023-3184
dfn-cert: DFN-CERT-2023-3183
dfn-cert: DFN-CERT-2023-3182
dfn-cert: DFN-CERT-2023-3175

Medium (CVSS: 6.5) NVT: OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities (Terrapin Attack)
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.6 Installation path / port: /snap/core22/1612/usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.6 or later. Note: Client and Server implementations need to run a fixed version to mitigate the Terrapin flaw.
Affected Software/OS
... continues on next page ...

...continued from previous page ...
OpenBSD OpenSSH prior to version 9.6.
<p>Vulnerability Insight</p> <p>The following vulnerabilities exist:</p> <ul style="list-style-type: none"> - CVE-2023-48795: The SSH transport protocol with certain OpenSSH extensions allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a 'Terrapin attack'. - CVE-2023-51384: In ssh-agent certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys. - CVE-2023-51385: OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities (Terrapin Attack)</p> <p>OID:1.3.6.1.4.1.25623.1.0.118572</p> <p>Version used: 2024-03-15T05:06:15Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:openbsd:openssh:8.9p1</p> <p>Method: OpenSSH Detection Consolidation</p> <p>OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>References</p> <p>cve: CVE-2023-48795</p> <p>cve: CVE-2023-51384</p> <p>cve: CVE-2023-51385</p> <p>url: https://www.openssh.com/txt/release-9.6</p> <p>url: https://terrapin-attack.com</p> <p>url: https://vin01.github.io/piptagole/ssh/security/openssh/libssh/remote-code-e↵xecution/2023/12/20/openssh-proxycommand-libssh-rce.html</p> <p>cert-bund: WID-SEC-2025-0168</p> <p>cert-bund: WID-SEC-2025-0144</p> <p>cert-bund: WID-SEC-2025-0139</p> <p>cert-bund: WID-SEC-2024-3377</p> <p>cert-bund: WID-SEC-2024-3320</p> <p>cert-bund: WID-SEC-2024-3198</p> <p>cert-bund: WID-SEC-2024-3195</p> <p>cert-bund: WID-SEC-2024-3140</p> <p>cert-bund: WID-SEC-2024-1913</p> <p>cert-bund: WID-SEC-2024-1781</p>
... continues on next page ...

...continued from previous page ...

cert-bund: WID-SEC-2024-1701
 cert-bund: WID-SEC-2024-1656
 cert-bund: WID-SEC-2024-1655
 cert-bund: WID-SEC-2024-1643
 cert-bund: WID-SEC-2024-1642
 cert-bund: WID-SEC-2024-1639
 cert-bund: WID-SEC-2024-1637
 cert-bund: WID-SEC-2024-1630
 cert-bund: WID-SEC-2024-1474
 cert-bund: WID-SEC-2024-1248
 cert-bund: WID-SEC-2024-1228
 cert-bund: WID-SEC-2024-1186
 cert-bund: WID-SEC-2024-1082
 cert-bund: WID-SEC-2024-0899
 cert-bund: WID-SEC-2024-0892
 cert-bund: WID-SEC-2024-0889
 cert-bund: WID-SEC-2024-0885
 cert-bund: WID-SEC-2024-0874
 cert-bund: WID-SEC-2024-0869
 cert-bund: WID-SEC-2024-0578
 cert-bund: WID-SEC-2024-0564
 cert-bund: WID-SEC-2024-0523
 cert-bund: WID-SEC-2023-3182
 cert-bund: WID-SEC-2023-3174
 dfn-cert: DFN-CERT-2025-0294
 dfn-cert: DFN-CERT-2025-0173
 dfn-cert: DFN-CERT-2025-0165
 dfn-cert: DFN-CERT-2025-0024
 dfn-cert: DFN-CERT-2024-3171
 dfn-cert: DFN-CERT-2024-2818
 dfn-cert: DFN-CERT-2024-2759
 dfn-cert: DFN-CERT-2024-2741
 dfn-cert: DFN-CERT-2024-2682
 dfn-cert: DFN-CERT-2024-2602
 dfn-cert: DFN-CERT-2024-2573
 dfn-cert: DFN-CERT-2024-2392
 dfn-cert: DFN-CERT-2024-2210
 dfn-cert: DFN-CERT-2024-2209
 dfn-cert: DFN-CERT-2024-2194
 dfn-cert: DFN-CERT-2024-2169
 dfn-cert: DFN-CERT-2024-2048
 dfn-cert: DFN-CERT-2024-2030
 dfn-cert: DFN-CERT-2024-2028
 dfn-cert: DFN-CERT-2024-1930
 dfn-cert: DFN-CERT-2024-1895
 dfn-cert: DFN-CERT-2024-1869
 dfn-cert: DFN-CERT-2024-1868

...continues on next page ...

...continued from previous page ...	
dfn-cert:	DFN-CERT-2024-1865
dfn-cert:	DFN-CERT-2024-1862
dfn-cert:	DFN-CERT-2024-1854
dfn-cert:	DFN-CERT-2024-1846
dfn-cert:	DFN-CERT-2024-1817
dfn-cert:	DFN-CERT-2024-1794
dfn-cert:	DFN-CERT-2024-1715
dfn-cert:	DFN-CERT-2024-1698
dfn-cert:	DFN-CERT-2024-1688
dfn-cert:	DFN-CERT-2024-1655
dfn-cert:	DFN-CERT-2024-1600
dfn-cert:	DFN-CERT-2024-1443
dfn-cert:	DFN-CERT-2024-1442
dfn-cert:	DFN-CERT-2024-1413
dfn-cert:	DFN-CERT-2024-1382
dfn-cert:	DFN-CERT-2024-1380
dfn-cert:	DFN-CERT-2024-1373
dfn-cert:	DFN-CERT-2024-1260
dfn-cert:	DFN-CERT-2024-1259
dfn-cert:	DFN-CERT-2024-1108
dfn-cert:	DFN-CERT-2024-1061
dfn-cert:	DFN-CERT-2024-1029
dfn-cert:	DFN-CERT-2024-1003
dfn-cert:	DFN-CERT-2024-1000
dfn-cert:	DFN-CERT-2024-0896
dfn-cert:	DFN-CERT-2024-0779
dfn-cert:	DFN-CERT-2024-0762
dfn-cert:	DFN-CERT-2024-0744
dfn-cert:	DFN-CERT-2024-0698
dfn-cert:	DFN-CERT-2024-0633
dfn-cert:	DFN-CERT-2024-0619
dfn-cert:	DFN-CERT-2024-0618
dfn-cert:	DFN-CERT-2024-0616
dfn-cert:	DFN-CERT-2024-0597
dfn-cert:	DFN-CERT-2024-0545
dfn-cert:	DFN-CERT-2024-0526
dfn-cert:	DFN-CERT-2024-0491
dfn-cert:	DFN-CERT-2024-0480
dfn-cert:	DFN-CERT-2024-0451
dfn-cert:	DFN-CERT-2024-0440
dfn-cert:	DFN-CERT-2024-0420
dfn-cert:	DFN-CERT-2024-0388
dfn-cert:	DFN-CERT-2024-0343
dfn-cert:	DFN-CERT-2024-0306
dfn-cert:	DFN-CERT-2024-0299
dfn-cert:	DFN-CERT-2024-0285
dfn-cert:	DFN-CERT-2024-0267
...continues on next page ...	

...continued from previous page ...
dfn-cert: DFN-CERT-2024-0251
dfn-cert: DFN-CERT-2024-0215
dfn-cert: DFN-CERT-2024-0211
dfn-cert: DFN-CERT-2024-0164
dfn-cert: DFN-CERT-2024-0154
dfn-cert: DFN-CERT-2024-0101
dfn-cert: DFN-CERT-2024-0092
dfn-cert: DFN-CERT-2024-0088
dfn-cert: DFN-CERT-2024-0067
dfn-cert: DFN-CERT-2024-0063
dfn-cert: DFN-CERT-2024-0062
dfn-cert: DFN-CERT-2024-0024
dfn-cert: DFN-CERT-2024-0022
dfn-cert: DFN-CERT-2024-0013
dfn-cert: DFN-CERT-2023-3219
dfn-cert: DFN-CERT-2023-3218
dfn-cert: DFN-CERT-2023-3210
dfn-cert: DFN-CERT-2023-3201
dfn-cert: DFN-CERT-2023-3200
dfn-cert: DFN-CERT-2023-3195
dfn-cert: DFN-CERT-2023-3193
dfn-cert: DFN-CERT-2023-3191
dfn-cert: DFN-CERT-2023-3185
dfn-cert: DFN-CERT-2023-3184
dfn-cert: DFN-CERT-2023-3183
dfn-cert: DFN-CERT-2023-3182
dfn-cert: DFN-CERT-2023-3175

Medium (CVSS: 6.5) NVT: OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities (Terrapin Attack)
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.6 Installation path / port: /snap/core22/1612/usr/bin/ssh
... continues on next page ...

...continued from previous page ...
Solution: Solution type: VendorFix Update to version 9.6 or later. Note: Client and Server implementations need to run a fixed version to mitigate the Terrapin flaw.
Affected Software/OS OpenBSD OpenSSH prior to version 9.6.
Vulnerability Insight The following vulnerabilities exist: - CVE-2023-48795: The SSH transport protocol with certain OpenSSH extensions allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a 'Terrapin attack'. - CVE-2023-51384: In ssh-agent certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys. - CVE-2023-51385: OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities (Terrapin Attack) OID:1.3.6.1.4.1.25623.1.0.118572 Version used: 2024-03-15T05:06:15Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2023-48795 cve: CVE-2023-51384 cve: CVE-2023-51385 url: https://www.openssh.com/txt/release-9.6 url: https://terrapin-attack.com url: https://vin01.github.io/piptagole/ssh/security/openssh/libssh/remote-code-e ↪xecution/2023/12/20/openssh-proxycommand-libssh-rce.html cert-bund: WID-SEC-2025-0168
...continues on next page ...

...continued from previous page ...	
cert-bund:	WID-SEC-2025-0144
cert-bund:	WID-SEC-2025-0139
cert-bund:	WID-SEC-2024-3377
cert-bund:	WID-SEC-2024-3320
cert-bund:	WID-SEC-2024-3198
cert-bund:	WID-SEC-2024-3195
cert-bund:	WID-SEC-2024-3140
cert-bund:	WID-SEC-2024-1913
cert-bund:	WID-SEC-2024-1781
cert-bund:	WID-SEC-2024-1701
cert-bund:	WID-SEC-2024-1656
cert-bund:	WID-SEC-2024-1655
cert-bund:	WID-SEC-2024-1643
cert-bund:	WID-SEC-2024-1642
cert-bund:	WID-SEC-2024-1639
cert-bund:	WID-SEC-2024-1637
cert-bund:	WID-SEC-2024-1630
cert-bund:	WID-SEC-2024-1474
cert-bund:	WID-SEC-2024-1248
cert-bund:	WID-SEC-2024-1228
cert-bund:	WID-SEC-2024-1186
cert-bund:	WID-SEC-2024-1082
cert-bund:	WID-SEC-2024-0899
cert-bund:	WID-SEC-2024-0892
cert-bund:	WID-SEC-2024-0889
cert-bund:	WID-SEC-2024-0885
cert-bund:	WID-SEC-2024-0874
cert-bund:	WID-SEC-2024-0869
cert-bund:	WID-SEC-2024-0578
cert-bund:	WID-SEC-2024-0564
cert-bund:	WID-SEC-2024-0523
cert-bund:	WID-SEC-2023-3182
cert-bund:	WID-SEC-2023-3174
dfn-cert:	DFN-CERT-2025-0294
dfn-cert:	DFN-CERT-2025-0173
dfn-cert:	DFN-CERT-2025-0165
dfn-cert:	DFN-CERT-2025-0024
dfn-cert:	DFN-CERT-2024-3171
dfn-cert:	DFN-CERT-2024-2818
dfn-cert:	DFN-CERT-2024-2759
dfn-cert:	DFN-CERT-2024-2741
dfn-cert:	DFN-CERT-2024-2682
dfn-cert:	DFN-CERT-2024-2602
dfn-cert:	DFN-CERT-2024-2573
dfn-cert:	DFN-CERT-2024-2392
dfn-cert:	DFN-CERT-2024-2210
dfn-cert:	DFN-CERT-2024-2209
...continues on next page ...	

...continued from previous page ...	
dfn-cert:	DFN-CERT-2024-2194
dfn-cert:	DFN-CERT-2024-2169
dfn-cert:	DFN-CERT-2024-2048
dfn-cert:	DFN-CERT-2024-2030
dfn-cert:	DFN-CERT-2024-2028
dfn-cert:	DFN-CERT-2024-1930
dfn-cert:	DFN-CERT-2024-1895
dfn-cert:	DFN-CERT-2024-1869
dfn-cert:	DFN-CERT-2024-1868
dfn-cert:	DFN-CERT-2024-1865
dfn-cert:	DFN-CERT-2024-1862
dfn-cert:	DFN-CERT-2024-1854
dfn-cert:	DFN-CERT-2024-1846
dfn-cert:	DFN-CERT-2024-1817
dfn-cert:	DFN-CERT-2024-1794
dfn-cert:	DFN-CERT-2024-1715
dfn-cert:	DFN-CERT-2024-1698
dfn-cert:	DFN-CERT-2024-1688
dfn-cert:	DFN-CERT-2024-1655
dfn-cert:	DFN-CERT-2024-1600
dfn-cert:	DFN-CERT-2024-1443
dfn-cert:	DFN-CERT-2024-1442
dfn-cert:	DFN-CERT-2024-1413
dfn-cert:	DFN-CERT-2024-1382
dfn-cert:	DFN-CERT-2024-1380
dfn-cert:	DFN-CERT-2024-1373
dfn-cert:	DFN-CERT-2024-1260
dfn-cert:	DFN-CERT-2024-1259
dfn-cert:	DFN-CERT-2024-1108
dfn-cert:	DFN-CERT-2024-1061
dfn-cert:	DFN-CERT-2024-1029
dfn-cert:	DFN-CERT-2024-1003
dfn-cert:	DFN-CERT-2024-1000
dfn-cert:	DFN-CERT-2024-0896
dfn-cert:	DFN-CERT-2024-0779
dfn-cert:	DFN-CERT-2024-0762
dfn-cert:	DFN-CERT-2024-0744
dfn-cert:	DFN-CERT-2024-0698
dfn-cert:	DFN-CERT-2024-0633
dfn-cert:	DFN-CERT-2024-0619
dfn-cert:	DFN-CERT-2024-0618
dfn-cert:	DFN-CERT-2024-0616
dfn-cert:	DFN-CERT-2024-0597
dfn-cert:	DFN-CERT-2024-0545
dfn-cert:	DFN-CERT-2024-0526
dfn-cert:	DFN-CERT-2024-0491
dfn-cert:	DFN-CERT-2024-0480
...continues on next page ...	

...continued from previous page ...

dfn-cert: DFN-CERT-2024-0451
dfn-cert: DFN-CERT-2024-0440
dfn-cert: DFN-CERT-2024-0420
dfn-cert: DFN-CERT-2024-0388
dfn-cert: DFN-CERT-2024-0343
dfn-cert: DFN-CERT-2024-0306
dfn-cert: DFN-CERT-2024-0299
dfn-cert: DFN-CERT-2024-0285
dfn-cert: DFN-CERT-2024-0267
dfn-cert: DFN-CERT-2024-0251
dfn-cert: DFN-CERT-2024-0215
dfn-cert: DFN-CERT-2024-0211
dfn-cert: DFN-CERT-2024-0164
dfn-cert: DFN-CERT-2024-0154
dfn-cert: DFN-CERT-2024-0101
dfn-cert: DFN-CERT-2024-0092
dfn-cert: DFN-CERT-2024-0088
dfn-cert: DFN-CERT-2024-0067
dfn-cert: DFN-CERT-2024-0063
dfn-cert: DFN-CERT-2024-0062
dfn-cert: DFN-CERT-2024-0024
dfn-cert: DFN-CERT-2024-0022
dfn-cert: DFN-CERT-2024-0013
dfn-cert: DFN-CERT-2023-3219
dfn-cert: DFN-CERT-2023-3218
dfn-cert: DFN-CERT-2023-3210
dfn-cert: DFN-CERT-2023-3201
dfn-cert: DFN-CERT-2023-3200
dfn-cert: DFN-CERT-2023-3195
dfn-cert: DFN-CERT-2023-3193
dfn-cert: DFN-CERT-2023-3191
dfn-cert: DFN-CERT-2023-3185
dfn-cert: DFN-CERT-2023-3184
dfn-cert: DFN-CERT-2023-3183
dfn-cert: DFN-CERT-2023-3182
dfn-cert: DFN-CERT-2023-3175

Medium (CVSS: 6.5)

NVT: PHP < 7.4.31, 8.0.x < 8.0.24, 8.1.x < 8.1.11 Security Update - Linux

Product detection result

cpe:/a:php:php:7.2.34

Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

PHP is prone to multiple vulnerabilities.

... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.4.31 Installation path / port: /usr/bin/php7.2
Solution: Solution type: VendorFix Update to version 7.4.31, 8.0.24, 8.1.11 or later.
Affected Software/OS PHP versions prior to 7.4.31, 8.0.x prior to 8.0.24 and 8.1.x prior to 8.1.11.
Vulnerability Insight The following vulnerabilities exist: - CVE-2022-31628: The phar uncompressor code would recursively uncompress 'quines' gzip files, resulting in an infinite loop. - CVE-2022-31629: The vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a '__Host-' or '__Secure-' cookie by PHP applications.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.4.31, 8.0.x < 8.0.24, 8.1.x < 8.1.11 Security Update - Linux OID:1.3.6.1.4.1.25623.1.0.104331 Version used: 2023-10-19T05:05:21Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2022-31628 cve: CVE-2022-31629 url: https://www.php.net/ChangeLog-7.php#7.4.31 url: https://www.php.net/ChangeLog-8.php#8.0.24 url: https://www.php.net/ChangeLog-8.php#8.1.11 url: https://bugs.php.net/bug.php?id=81726 url: https://bugs.php.net/bug.php?id=81727 cert-bund: WID-SEC-2023-1737 cert-bund: WID-SEC-2023-0561
... continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2022-1567
dfn-cert: DFN-CERT-2024-1192
dfn-cert: DFN-CERT-2023-1600
dfn-cert: DFN-CERT-2023-0422
dfn-cert: DFN-CERT-2022-2869
dfn-cert: DFN-CERT-2022-2639
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2022-2598
dfn-cert: DFN-CERT-2022-2523
dfn-cert: DFN-CERT-2022-2337
dfn-cert: DFN-CERT-2022-2157

Medium (CVSS: 6.5) NVT: Intel CPU Information Disclosure Vulnerability (INTEL-SA-00698, Hertzbleed)
Summary The Intel CPU on the remote host might be prone to an information disclosure vulnerability dubbed 'Hertzbleed'.
Quality of Detection (QoD): 1%
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution: Solution type: Mitigation Intel is providing Software Guidance for cryptographic implementations. Cryptographic developers may choose to follow the guidance to harden their libraries and applications against frequency throttling information disclosure.
Vulnerability Insight Observable behavioral in power management throttling for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via network access.
Vulnerability Detection Method Checks if the remote host is using an Intel CPU. Details: Intel CPU Information Disclosure Vulnerability (INTEL-SA-00698, Hertzbleed) OID:1.3.6.1.4.1.25623.1.0.104264 Version used: 2022-08-03T10:11:15Z
References cve: CVE-2022-24436 url: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00698.html url: https://www.intel.com/content/www/us/en/developer/articles/technical/softwa ... continues on next page ...

...continued from previous page ...
↔re-security-guidance/technical-documentation/frequency-throttling-side-channel ↔-guidance.html url: https://www.hertzbleed.com cert-bund: WID-SEC-2022-0333 dfn-cert: DFN-CERT-2022-1334

Medium (CVSS: 6.5) NVT: OpenSSL Vector Register Corruption Vulnerability (20240109)
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a vector register corruption vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.13 Installation path / port: /usr/bin/openssl
Impact If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences.
Solution: Solution type: VendorFix Update to version 3.0.13, 3.1.5, 3.2.1 or later.
Affected Software/OS OpenSSL versions 3.0, 3.1 and 3.2 on PowerPC CPU based platforms if the CPU provides vector instructions.
Vulnerability Insight The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL Vector Register Corruption Vulnerability (20240109)
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.114253 Version used: 2024-01-30T14:37:03Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2023-6129 url: https://www.openssl.org/news/secadv/20240109.txt cert-bund: WID-SEC-2025-0168 cert-bund: WID-SEC-2024-1657 cert-bund: WID-SEC-2024-1656 cert-bund: WID-SEC-2024-1638 cert-bund: WID-SEC-2024-1637 cert-bund: WID-SEC-2024-1488 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0894 cert-bund: WID-SEC-2024-0769 cert-bund: WID-SEC-2024-0034 dfn-cert: DFN-CERT-2025-0173 dfn-cert: DFN-CERT-2024-2981 dfn-cert: DFN-CERT-2024-1865 dfn-cert: DFN-CERT-2024-1856 dfn-cert: DFN-CERT-2024-1846 dfn-cert: DFN-CERT-2024-1166 dfn-cert: DFN-CERT-2024-1067 dfn-cert: DFN-CERT-2024-1002 dfn-cert: DFN-CERT-2024-0531 dfn-cert: DFN-CERT-2024-0296 dfn-cert: DFN-CERT-2024-0253 dfn-cert: DFN-CERT-2024-0175 dfn-cert: DFN-CERT-2024-0058
Medium (CVSS: 6.5) NVT: OpenSSL Vector Register Corruption Vulnerability (20240109)
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary
... continues on next page ...

...continued from previous page ...
OpenSSL is prone to a vector register corruption vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.13 Installation path / port: /snap/core22/1748/usr/bin/openssl
Impact If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences.
Solution: Solution type: VendorFix Update to version 3.0.13, 3.1.5, 3.2.1 or later.
Affected Software/OS OpenSSL versions 3.0, 3.1 and 3.2 on PowerPC CPU based platforms if the CPU provides vector instructions.
Vulnerability Insight The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL Vector Register Corruption Vulnerability (20240109) OID: 1.3.6.1.4.1.25623.1.0.114253 Version used: 2024-01-30T14:37:03Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2023-6129 url: https://www.openssl.org/news/secadv/20240109.txt cert-bund: WID-SEC-2025-0168 cert-bund: WID-SEC-2024-1657 cert-bund: WID-SEC-2024-1656 cert-bund: WID-SEC-2024-1638
... continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2024-1637
cert-bund: WID-SEC-2024-1488
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0894
cert-bund: WID-SEC-2024-0769
cert-bund: WID-SEC-2024-0034
dfn-cert: DFN-CERT-2025-0173
dfn-cert: DFN-CERT-2024-2981
dfn-cert: DFN-CERT-2024-1865
dfn-cert: DFN-CERT-2024-1856
dfn-cert: DFN-CERT-2024-1846
dfn-cert: DFN-CERT-2024-1166
dfn-cert: DFN-CERT-2024-1067
dfn-cert: DFN-CERT-2024-1002
dfn-cert: DFN-CERT-2024-0531
dfn-cert: DFN-CERT-2024-0296
dfn-cert: DFN-CERT-2024-0253
dfn-cert: DFN-CERT-2024-0175
dfn-cert: DFN-CERT-2024-0058

Medium (CVSS: 6.5) NVT: OpenSSL Vector Register Corruption Vulnerability (20240109)
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a vector register corruption vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.13 Installation path / port: /snap/core22/1612/usr/bin/openssl
Impact If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences.
Solution: Solution type: VendorFix Update to version 3.0.13, 3.1.5, 3.2.1 or later.
... continues on next page ...

...continued from previous page ...
Affected Software/OS OpenSSL versions 3.0, 3.1 and 3.2 on PowerPC CPU based platforms if the CPU provides vector instructions.
Vulnerability Insight The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL Vector Register Corruption Vulnerability (20240109) OID:1.3.6.1.4.1.25623.1.0.114253 Version used: 2024-01-30T14:37:03Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2023-6129 url: https://www.openssl.org/news/secadv/20240109.txt cert-bund: WID-SEC-2025-0168 cert-bund: WID-SEC-2024-1657 cert-bund: WID-SEC-2024-1656 cert-bund: WID-SEC-2024-1638 cert-bund: WID-SEC-2024-1637 cert-bund: WID-SEC-2024-1488 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0894 cert-bund: WID-SEC-2024-0769 cert-bund: WID-SEC-2024-0034 dfn-cert: DFN-CERT-2025-0173 dfn-cert: DFN-CERT-2024-2981 dfn-cert: DFN-CERT-2024-1865 dfn-cert: DFN-CERT-2024-1856 dfn-cert: DFN-CERT-2024-1846 dfn-cert: DFN-CERT-2024-1166 dfn-cert: DFN-CERT-2024-1067 dfn-cert: DFN-CERT-2024-1002 dfn-cert: DFN-CERT-2024-0531 dfn-cert: DFN-CERT-2024-0296
...continues on next page ...

...continued from previous page ...	
dfn-cert: DFN-CERT-2024-0253	
dfn-cert: DFN-CERT-2024-0175	
dfn-cert: DFN-CERT-2024-0058	
Medium (CVSS: 6.4) NVT: NTP <= 4.2.8p15 Multiple Vulnerabilities	
Product detection result cpe:/a:ntp:ntp:4.2.8:p15 Detected by NTPd Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.25623.1.0.80 ↪0407)	
Summary NTP is prone to multiple vulnerabilities.	
Quality of Detection (QoD): 30%	
Vulnerability Detection Result Installed version: 4.2.8p15 Fixed version: 4.2.8p16 Installation path / port: /usr/sbin/ntpd	
Solution: Solution type: VendorFix Update to version 4.2.8p16 or later.	
Affected Software/OS NTPd version 4.2.8p15 and prior.	
Vulnerability Insight The following flaws exist: <ul style="list-style-type: none"> - CVE-2023-26551: mstolfp in libntp/mstolfp.c has an out-of-bounds write in the cp<cpdec while loop. An adversary may be able to attack a client ntpq process, but cannot attack ntpd. - CVE-2023-26552: mstolfp in libntp/mstolfp.c has an out-of-bounds write when adding a decimal point. An adversary may be able to attack a client ntpq process, but cannot attack ntpd. - CVE-2023-26553: mstolfp in libntp/mstolfp.c has an out-of-bounds write when copying the trailing number. An adversary may be able to attack a client ntpq process, but cannot attack ntpd. - CVE-2023-26554: mstolfp in libntp/mstolfp.c has an out-of-bounds write when adding a '\0' character. An adversary may be able to attack a client ntpq process, but cannot attack ntpd. - CVE-2023-26555: praecis_parse in ntpd/refclock_palisade.c has an out-of-bounds write. Any attack method would be complex, e.g., with a manipulated GPS receiver. 	
... continues on next page ...	

...continued from previous page ...
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: NTP <= 4.2.8p15 Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.104669 Version used: 2024-02-20T05:05:48Z
Product Detection Result Product: cpe:/a:ntp:ntp:4.2.8:p15 Method: NTPd Detection (Linux/Unix SSH Login) OID: 1.3.6.1.4.1.25623.1.0.800407)
References cve: CVE-2023-26551 cve: CVE-2023-26552 cve: CVE-2023-26553 cve: CVE-2023-26554 cve: CVE-2023-26555 url: https://www.ntp.org/support/securitynotice/4_2_8p16-release-announcement/ url: https://www.ntp.org/support/securitynotice/#428p16 url: https://github.com/spwpun/ntp-4.2.8p15-cves url: https://github.com/spwpun/ntp-4.2.8p15-cves/issues/1 cert-bund: WID-SEC-2023-0938 dfn-cert: DFN-CERT-2023-2941 dfn-cert: DFN-CERT-2023-2491 dfn-cert: DFN-CERT-2023-2490 dfn-cert: DFN-CERT-2023-1295 dfn-cert: DFN-CERT-2023-1196 dfn-cert: DFN-CERT-2023-1078
Medium (CVSS: 5.9) NVT: OpenSSL 3.0 <= 3.0.8, 3.1.0 DoS Vulnerability
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.9 Installation
... continues on next page ...

...continued from previous page...	
path / port:	/snap/core22/1748/usr/bin/openssl
Impact Applications that use the AES-XTS algorithm on the 64 bit ARM platform can crash in rare circumstances. The AES-XTS algorithm is usually used for disk encryption. The AES-XTS cipher decryption implementation for 64 bit ARM platform will read past the end of the ciphertext buffer if the ciphertext size is 4 mod 5 in 16 byte blocks, e.g. 144 bytes or 1024 bytes. If the memory after the ciphertext buffer is unmapped, this will trigger a crash which results in a denial of service. If an attacker can control the size and location of the ciphertext buffer being decrypted by an application using AES-XTS on 64 bit ARM, the application is affected. This is fairly unlikely making this issue a Low severity one.	
Solution: Solution type: VendorFix Update to version 3.0.9, 3.1.1 or later.	
Affected Software/OS OpenSSL versions 3.0.0 through 3.0.8 and 3.1.0 on 64 bit ARM platforms.	
Vulnerability Insight The AES-XTS cipher decryption implementation for 64 bit ARM platform contains a bug that could cause it to read past the input buffer, leading to a crash.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL 3.0 <= 3.0.8, 3.1.0 DoS Vulnerability OID:1.3.6.1.4.1.25623.1.0.104696 Version used: 2023-10-13T05:06:10Z	
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)	
References cve: CVE-2023-1255 url: https://www.openssl.org/news/secadv/20230420.txt cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2023-1614 cert-bund: WID-SEC-2023-1053 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-1067 dfn-cert: DFN-CERT-2023-1428 dfn-cert: DFN-CERT-2023-1332	
... continues on next page ...	

...continued from previous page ...
dfn-cert: DFN-CERT-2023-1246 dfn-cert: DFN-CERT-2023-1233 dfn-cert: DFN-CERT-2023-0929
Medium (CVSS: 5.9) NVT: OpenSSL 3.0 <= 3.0.8, 3.1.0 DoS Vulnerability
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.9 Installation path / port: /usr/bin/openssl
Impact Applications that use the AES-XTS algorithm on the 64 bit ARM platform can crash in rare circumstances. The AES-XTS algorithm is usually used for disk encryption. The AES-XTS cipher decryption implementation for 64 bit ARM platform will read past the end of the ciphertext buffer if the ciphertext size is 4 mod 5 in 16 byte blocks, e.g. 144 bytes or 1024 bytes. If the memory after the ciphertext buffer is unmapped, this will trigger a crash which results in a denial of service. If an attacker can control the size and location of the ciphertext buffer being decrypted by an application using AES-XTS on 64 bit ARM, the application is affected. This is fairly unlikely making this issue a Low severity one.
Solution: Solution type: VendorFix Update to version 3.0.9, 3.1.1 or later.
Affected Software/OS OpenSSL versions 3.0.0 through 3.0.8 and 3.1.0 on 64 bit ARM platforms.
Vulnerability Insight The AES-XTS cipher decryption implementation for 64 bit ARM platform contains a bug that could cause it to read past the input buffer, leading to a crash.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL 3.0 <= 3.0.8, 3.1.0 DoS Vulnerability OID:1.3.6.1.4.1.25623.1.0.104696 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2023-1255 url: https://www.openssl.org/news/secadv/20230420.txt cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2023-1614 cert-bund: WID-SEC-2023-1053 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-1067 dfn-cert: DFN-CERT-2023-1428 dfn-cert: DFN-CERT-2023-1332 dfn-cert: DFN-CERT-2023-1246 dfn-cert: DFN-CERT-2023-1233 dfn-cert: DFN-CERT-2023-0929

Medium (CVSS: 5.9) NVT: PHP < 7.3.29 Multiple Vulnerabilities (Jul 2021) - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.3.29 Installation path / port: /usr/bin/php7.2
Solution: Solution type: VendorFix
... continues on next page ...

...continued from previous page ...
Update to version 7.3.29 or later.
Affected Software/OS PHP versions prior to 7.3.29.
Vulnerability Insight The following flaws exist: - CVE-2021-21705: SSRF bypass in FILTER_VALIDATE_URL. - CVE-2021-21704: Stack buffer overflow in firebird_info_cb. - CVE-2021-21704: SIGSEGV in firebird_handle_doer. - CVE-2021-21704: SIGSEGV in firebird_stmt_execute. - CVE-2021-21704: Crash while parsing blob data in firebird_fetch_blob.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.3.29 Multiple Vulnerabilities (Jul 2021) - Linux OID:1.3.6.1.4.1.25623.1.0.117524 Version used: 2023-10-20T16:09:12Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2021-21704 cve: CVE-2021-21705 url: https://www.php.net/ChangeLog-7.php#7.3.29 url: http://bugs.php.net/81122 url: http://bugs.php.net/76448 url: http://bugs.php.net/76449 url: http://bugs.php.net/76450 url: http://bugs.php.net/76452 cert-bund: WID-SEC-2023-1737 cert-bund: WID-SEC-2022-1577 cert-bund: WID-SEC-2022-0624 cert-bund: CB-K21/0705 dfn-cert: DFN-CERT-2023-1600 dfn-cert: DFN-CERT-2022-2639 dfn-cert: DFN-CERT-2022-2638 dfn-cert: DFN-CERT-2022-1046 dfn-cert: DFN-CERT-2021-2185 dfn-cert: DFN-CERT-2021-1676 dfn-cert: DFN-CERT-2021-1645 dfn-cert: DFN-CERT-2021-1627
... continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2021-1509 dfn-cert: DFN-CERT-2021-1453 dfn-cert: DFN-CERT-2021-1419
Medium (CVSS: 5.9) NVT: Samba 4.1 < 4.17.1 Improper Authentication (CVE-2021-20251)
Product detection result cpe:/a:samba:samba:4.15.13 Detected by Samba Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800403)
Summary Samba is prone to an improper authentication vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 4.15.13 Fixed version: 4.17.1 Installation path / port: /usr/sbin/smbd
Solution: Solution type: VendorFix Update to version 4.17.1 or later.
Affected Software/OS Samba version 4.1 through 4.17.1.
Vulnerability Insight By making bad password count handling atomic, we ensure only one failed authorisation attempt can get through at a time, and refuse excess login attempts made to the same server.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Samba 4.1 < 4.17.1 Improper Authentication (CVE-2021-20251) OID:1.3.6.1.4.1.25623.1.0.126184 Version used: 2023-10-19T05:05:21Z
Product Detection Result Product: cpe:/a:samba:samba:4.15.13 Method: Samba Version Detection OID: 1.3.6.1.4.1.25623.1.0.800403)
... continues on next page ...

...continued from previous page ...

References

cve: CVE-2021-20251
 url: <https://www.samba.org/samba/history/samba-4.17.1.html>
 url: https://bugzilla.samba.org/show_bug.cgi?id=14611
 cert-bund: WID-SEC-2022-1799
 dfn-cert: DFN-CERT-2023-0201
 dfn-cert: DFN-CERT-2023-0199
 dfn-cert: DFN-CERT-2023-0176
 dfn-cert: DFN-CERT-2023-0153

Medium (CVSS: 5.9)

NVT: Apache HTTP Server 2.4.17 - 2.4.57 DoS Vulnerability - Linux

Product detection result

cpe:/a:apache:http_server:2.4.52
 Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
 ↪.0.117232)

Summary

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

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 2.4.52
 Fixed version: 2.4.58
 Installation
 path / port: /usr/sbin/apache2

Solution:

Solution type: VendorFix
 Update to version 2.4.58 or later.

Affected Software/OS

Apache HTTP Server version 2.4.17 through 2.4.57.

Vulnerability Insight

When a HTTP/2 stream was reset (RST frame) by a client, there was a time window where the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.

... continues on next page ...

...continued from previous page ...
<p>This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During 'normal' HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server 2.4.17 - 2.4.57 DoS Vulnerability - Linux OID:1.3.6.1.4.1.25623.1.0.100310 Version used: 2024-08-02T05:05:39Z</p>
<p>Product Detection Result Product: cpe:/a:apache:http_server:2.4.52 Method: Apache HTTP Server Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117232)</p>
<p>References cve: CVE-2023-45802 url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.58 url: https://www.openwall.com/lists/oss-security/2023/10/19/6 url: https://github.com/icing/blog/blob/main/h2-rapid-reset.md cert-bund: WID-SEC-2024-0769 cert-bund: WID-SEC-2023-2917 cert-bund: WID-SEC-2023-2712 dfn-cert: DFN-CERT-2024-2968 dfn-cert: DFN-CERT-2024-1411 dfn-cert: DFN-CERT-2024-1335 dfn-cert: DFN-CERT-2024-1152 dfn-cert: DFN-CERT-2024-1010 dfn-cert: DFN-CERT-2023-3071 dfn-cert: DFN-CERT-2023-2596 dfn-cert: DFN-CERT-2023-2583</p>
<p>Medium (CVSS: 5.9) NVT: OpenSSL 3.0 <= 3.0.8, 3.1.0 DoS Vulnerability</p>
<p>Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
<p>Summary OpenSSL is prone to a denial of service (DoS) vulnerability.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result</p>
<p>... continues on next page ...</p>

...continued from previous page ...	
Installed version:	3.0.2
Fixed version:	3.0.9
Installation	
path / port:	/snap/core22/1612/usr/bin/openssl
Impact Applications that use the AES-XTS algorithm on the 64 bit ARM platform can crash in rare circumstances. The AES-XTS algorithm is usually used for disk encryption. The AES-XTS cipher decryption implementation for 64 bit ARM platform will read past the end of the ciphertext buffer if the ciphertext size is 4 mod 5 in 16 byte blocks, e.g. 144 bytes or 1024 bytes. If the memory after the ciphertext buffer is unmapped, this will trigger a crash which results in a denial of service. If an attacker can control the size and location of the ciphertext buffer being decrypted by an application using AES-XTS on 64 bit ARM, the application is affected. This is fairly unlikely making this issue a Low severity one.	
Solution: Solution type: VendorFix Update to version 3.0.9, 3.1.1 or later.	
Affected Software/OS OpenSSL versions 3.0.0 through 3.0.8 and 3.1.0 on 64 bit ARM platforms.	
Vulnerability Insight The AES-XTS cipher decryption implementation for 64 bit ARM platform contains a bug that could cause it to read past the input buffer, leading to a crash.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL 3.0 <= 3.0.8, 3.1.0 DoS Vulnerability OID:1.3.6.1.4.1.25623.1.0.104696 Version used: 2023-10-13T05:06:10Z	
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)	
References cve: CVE-2023-1255 url: https://www.openssl.org/news/secadv/20230420.txt cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2023-1614 cert-bund: WID-SEC-2023-1053 dfn-cert: DFN-CERT-2024-1799	
... continues on next page ...	

...continued from previous page ...
dfn-cert: DFN-CERT-2024-1067
dfn-cert: DFN-CERT-2023-1428
dfn-cert: DFN-CERT-2023-1332
dfn-cert: DFN-CERT-2023-1246
dfn-cert: DFN-CERT-2023-1233
dfn-cert: DFN-CERT-2023-0929

Medium (CVSS: 5.8) NVT: PHP < 8.1.28, 8.2.x < 8.2.18, 8.3.x < 8.3.6 Security Update (GHSA-h746-cjrr-wfmr) - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to a vulnerability in password_verify.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 8.1.28 Installation path / port: /usr/bin/php7.2
Solution: Solution type: VendorFix Update to version 8.1.28, 8.2.18, 8.3.6 or later.
Affected Software/OS PHP prior to version 8.1.28, version 8.2.x through 8.2.17 and 8.3.x through 8.3.5.
Vulnerability Insight If a password stored with password_hash starts with a null byte (\x00), testing a blank string as the password via password_verify will incorrectly return true. If a user were able to create a password with a leading null byte (unlikely, but syntactically valid), an attacker could trivially compromise the victim's account by attempting to sign in with a blank string.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 8.1.28, 8.2.x < 8.2.18, 8.3.x < 8.3.6 Security Update (GHSA-h746-cjrr-wfm. ↪...
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.152118 Version used: 2024-04-16T05:05:31Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2024-3096 url: https://github.com/php/php-src/security/advisories/GHSA-h746-cjrr-wfmr url: https://www.php.net/ChangeLog-8.php#8.1.28 url: https://www.php.net/ChangeLog-8.php#8.2.18 url: https://www.php.net/ChangeLog-8.php#8.3.6 cert-bund: WID-SEC-2024-0867 dfn-cert: DFN-CERT-2024-3330 dfn-cert: DFN-CERT-2024-3329 dfn-cert: DFN-CERT-2024-1574 dfn-cert: DFN-CERT-2024-1192 dfn-cert: DFN-CERT-2024-1132 dfn-cert: DFN-CERT-2024-1115 dfn-cert: DFN-CERT-2024-0993 dfn-cert: DFN-CERT-2024-0962

Medium (CVSS: 5.6) NVT: Intel CPU Information Disclosure Vulnerability (INTEL-SA-00330)
Summary The Intel CPU on the remote host might be prone to an information disclosure vulnerability.
Quality of Detection (QoD): 1%
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution: Solution type: Mitigation This potential vulnerability is mitigated by using Virtual Machine Manager with the L1TF mitigations applied. For more information see L1TF [link moved to references]. Intel is not recommending any new or additional mitigations for Operating Systems. Additional technical details about this vulnerability can be found at:link moved to references> link moved to refer Additional Advisory Guidance on CVE-2020-0550 available here [link moved to references].
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
Improper data forwarding in some data cache for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
Vulnerability Detection Method Checks if the remote host is using an Intel CPU. Details: Intel CPU Information Disclosure Vulnerability (INTEL-SA-00330) OID:1.3.6.1.4.1.25623.1.0.104263 Version used: 2022-08-03T10:11:15Z
References cve: CVE-2020-0550 url: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00330.html url: https://software.intel.com/security-software-guidance/processors-affected-transient-execution-attack-mitigation-product-cpu-model url: https://www.intel.com/content/www/us/en/architecture-and-technology/l1tf.html url: https://software.intel.com/security-software-guidance/insights/deep-dive-snooop-assisted-l1-data-sampling url: https://software.intel.com/content/www/us/en/develop/topics/software-security-guidance.html url: https://docs.kernel.org/admin-guide/hw-vuln/l1d_flush.html dfn-cert: DFN-CERT-2020-0506

Medium (CVSS: 5.5) NVT: OpenSSL DoS Vulnerability (20240125) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.13 Installation path / port: /usr/bin/openssl
Impact Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly.
... continues on next page ...

...continued from previous page ...
Solution: Solution type: VendorFix Update to version 1.0.2zj, 1.1.1x, 3.0.13, 3.1.5, 3.2.1 or later.
Affected Software/OS OpenSSL versions 1.0.2, 1.1.1, 3.0, 3.1 and 3.2.
Vulnerability Insight Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential DoS attack.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20240125) - Linux OID:1.3.6.1.4.1.25623.1.0.114307 Version used: 2024-02-05T05:05:38Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2024-0727 url: https://www.openssl.org/news/secadv/20240125.txt cert-bund: WID-SEC-2025-0225 cert-bund: WID-SEC-2024-3377 cert-bund: WID-SEC-2024-3222 cert-bund: WID-SEC-2024-2112 cert-bund: WID-SEC-2024-1696 cert-bund: WID-SEC-2024-1488 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0769 cert-bund: WID-SEC-2024-0181 dfn-cert: DFN-CERT-2024-2981 dfn-cert: DFN-CERT-2024-2884 dfn-cert: DFN-CERT-2024-2795 dfn-cert: DFN-CERT-2024-2745 dfn-cert: DFN-CERT-2024-2451 dfn-cert: DFN-CERT-2024-1867 dfn-cert: DFN-CERT-2024-1166 dfn-cert: DFN-CERT-2024-1011
... continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2024-0764
dfn-cert: DFN-CERT-2024-0539
dfn-cert: DFN-CERT-2024-0531
dfn-cert: DFN-CERT-2024-0374
dfn-cert: DFN-CERT-2024-0296
dfn-cert: DFN-CERT-2024-0225

Medium (CVSS: 5.5) NVT: OpenSSL DoS Vulnerability (20240125) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.13 Installation path / port: /snap/core22/1748/usr/bin/openssl
Impact Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly.
Solution: Solution type: VendorFix Update to version 1.0.2zj, 1.1.1x, 3.0.13, 3.1.5, 3.2.1 or later.
Affected Software/OS OpenSSL versions 1.0.2, 1.1.1, 3.0, 3.1 and 3.2.
Vulnerability Insight Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential DoS attack.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20240125) - Linux OID:1.3.6.1.4.1.25623.1.0.114307
... continues on next page ...

...continued from previous page ...
Version used: 2024-02-05T05:05:38Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2024-0727 url: https://www.openssl.org/news/secadv/20240125.txt cert-bund: WID-SEC-2025-0225 cert-bund: WID-SEC-2024-3377 cert-bund: WID-SEC-2024-3222 cert-bund: WID-SEC-2024-2112 cert-bund: WID-SEC-2024-1696 cert-bund: WID-SEC-2024-1488 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0769 cert-bund: WID-SEC-2024-0181 dfn-cert: DFN-CERT-2024-2981 dfn-cert: DFN-CERT-2024-2884 dfn-cert: DFN-CERT-2024-2795 dfn-cert: DFN-CERT-2024-2745 dfn-cert: DFN-CERT-2024-2451 dfn-cert: DFN-CERT-2024-1867 dfn-cert: DFN-CERT-2024-1166 dfn-cert: DFN-CERT-2024-1011 dfn-cert: DFN-CERT-2024-0764 dfn-cert: DFN-CERT-2024-0539 dfn-cert: DFN-CERT-2024-0531 dfn-cert: DFN-CERT-2024-0374 dfn-cert: DFN-CERT-2024-0296 dfn-cert: DFN-CERT-2024-0225
Medium (CVSS: 5.5) NVT: PHP < 8.0.22, 8.1.x < 8.1.9 Security Update - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary
... continues on next page ...

...continued from previous page ...
PHP is prone to a buffer overflow vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 8.0.22/8.1.9/8.2.0 Installation path / port: /usr/bin/php7.2
Solution: Solution type: VendorFix Update to version 8.0.22, 8.1.9, 8.2.0 or later.
Affected Software/OS PHP versions prior to 8.0.22 and 8.1.x prior to 8.1.9.
Vulnerability Insight Fixed potential overflow for the builtin server via the PHP_CLI_SERVER_WORKERS environment variable.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 8.0.22, 8.1.x < 8.1.9 Security Update - Linux OID:1.3.6.1.4.1.25623.1.0.104644 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2022-4900 url: https://www.php.net/ChangeLog-8.php#8.2.0 url: https://www.php.net/ChangeLog-8.php#8.1.9 url: https://www.php.net/ChangeLog-8.php#8.0.22 url: https://github.com/php/php-src/issues/8989 url: https://github.com/php/php-src/pull/9000 url: https://github.com/php/php-src/commit/789a37f14405e2d1a05a76c9fb4ed2d49d458 ↪0d5 url: https://bugzilla.redhat.com/show_bug.cgi?id=2179880 cert-bund: WID-SEC-2023-0695 dfn-cert: DFN-CERT-2024-2707 dfn-cert: DFN-CERT-2024-1132
... continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2023-0681
Medium (CVSS: 5.5) NVT: SQLite < 3.43.2 DoS Vulnerability
Product detection result cpe:/a:sqlite:sqlite:3.37.2 Detected by SQLite Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.25623.1.0.↵113789)
Summary SQLite is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.37.2 Fixed version: 3.43.2 Installation path / port: /usr/bin/sqlite3
Impact This flaw allows a local attacker to leverage a victim to pass specially crafted malicious input to the application, potentially causing a crash and leading to a denial of service.
Solution: Solution type: VendorFix Update to version 3.43.2 or later.
Affected Software/OS SQLite prior to version 3.43.2.
Vulnerability Insight A heap use-after-free issue has been identified in the jsonParseAddNodeArray() function in sqlite3.c.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: SQLite < 3.43.2 DoS Vulnerability OID:1.3.6.1.4.1.25623.1.0.126591 Version used: 2024-06-26T05:05:39Z
Product Detection Result Product: cpe:/a:sqlite:sqlite:3.37.2 ... continues on next page ...

...continued from previous page ...
Method: SQLite Detection (Linux/Unix SSH Login) OID: 1.3.6.1.4.1.25623.1.0.113789)
References cve: CVE-2024-0232 url: https://sqlite.org/forum/forumpost/4aa381993a cert-bund: WID-SEC-2025-0135 cert-bund: WID-SEC-2024-3222 cert-bund: WID-SEC-2024-3192 cert-bund: WID-SEC-2024-1655 cert-bund: WID-SEC-2024-1643 dfn-cert: DFN-CERT-2024-2745 dfn-cert: DFN-CERT-2024-1862 dfn-cert: DFN-CERT-2024-0467

Medium (CVSS: 5.5) NVT: OpenSSL DoS Vulnerability (20240125) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.13 Installation path / port: /snap/core22/1612/usr/bin/openssl
Impact Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly.
Solution: Solution type: VendorFix Update to version 1.0.2zj, 1.1.1x, 3.0.13, 3.1.5, 3.2.1 or later.
Affected Software/OS OpenSSL versions 1.0.2, 1.1.1, 3.0, 3.1 and 3.2.
... continues on next page ...

...continued from previous page...

Vulnerability Insight

Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential DoS attack.

Vulnerability Detection Method

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

Details: OpenSSL DoS Vulnerability (20240125) - Linux

OID:1.3.6.1.4.1.25623.1.0.114307

Version used: 2024-02-05T05:05:38Z

Product Detection Result

Product: cpe:/a:openssl:openssl:3.0.2

Method: OpenSSL Detection Consolidation

OID: 1.3.6.1.4.1.25623.1.0.145462)

References

cve: CVE-2024-0727

url: <https://www.openssl.org/news/secadv/20240125.txt>

cert-bund: WID-SEC-2025-0225

cert-bund: WID-SEC-2024-3377

cert-bund: WID-SEC-2024-3222

cert-bund: WID-SEC-2024-2112

cert-bund: WID-SEC-2024-1696

cert-bund: WID-SEC-2024-1488

cert-bund: WID-SEC-2024-1307

cert-bund: WID-SEC-2024-1248

cert-bund: WID-SEC-2024-1226

cert-bund: WID-SEC-2024-0769

cert-bund: WID-SEC-2024-0181

dfn-cert: DFN-CERT-2024-2981

dfn-cert: DFN-CERT-2024-2884

dfn-cert: DFN-CERT-2024-2795

dfn-cert: DFN-CERT-2024-2745

dfn-cert: DFN-CERT-2024-2451

dfn-cert: DFN-CERT-2024-1867

dfn-cert: DFN-CERT-2024-1166

dfn-cert: DFN-CERT-2024-1011

dfn-cert: DFN-CERT-2024-0764

dfn-cert: DFN-CERT-2024-0539

dfn-cert: DFN-CERT-2024-0531

dfn-cert: DFN-CERT-2024-0374

dfn-cert: DFN-CERT-2024-0296

dfn-cert: DFN-CERT-2024-0225

Medium (CVSS: 5.5) NVT: Intel CPU Information Disclosure Vulnerability (INTEL-SA-00657, AEPIC)
Summary The Intel CPU on the remote host might be prone to an information disclosure vulnerability dubbed 'AEPIC'.
Quality of Detection (QoD): 1%
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution: Solution type: VendorFix Intel recommends that users of affected Intel(R) Processors update to the latest version firmware provided by the system manufacturer that addresses these issues. In addition, Intel will be releasing Intel(R) SGX SDK updates soon after public embargo is lifted. Intel has released microcode updates for the affected Intel(R) Processors that are currently supported on the public github repository. Please see details below on access to the microcode: GitHub*: Public Github: [link moved to references]
Vulnerability Insight Improper isolation of shared resources in some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.
Vulnerability Detection Method Checks if the remote host is using an Intel CPU. Details: Intel CPU Information Disclosure Vulnerability (INTEL-SA-00657, AEPIC) OID:1.3.6.1.4.1.25623.1.0.104293 Version used: 2023-10-18T05:05:17Z
References cve: CVE-2022-21233 url: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00657.html url: https://aepicleak.com url: https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2023-1432 cert-bund: WID-SEC-2022-0986 dfn-cert: DFN-CERT-2023-0735 dfn-cert: DFN-CERT-2022-1787

Medium (CVSS: 5.3) NVT: OpenSSL: AES OCB fails to encrypt some bytes (CVE-2022-2097) - Linux
...
... continues on next page ...

...continued from previous page ...
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.5 Installation path / port: /usr/bin/openssl
Solution: Solution type: VendorFix Update to version 1.1.1q, 3.0.5 or later.
Affected Software/OS OpenSSL version 1.1.1 and 3.0.
Vulnerability Insight AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of 'in place' encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL: AES OCB fails to encrypt some bytes (CVE-2022-2097) - Linux OID:1.3.6.1.4.1.25623.1.0.148392 Version used: 2022-08-29T10:21:34Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2022-2097 url: https://www.openssl.org/news/secadv/20220705.txt
... continues on next page ...

...continued from previous page ...	
cert-bund:	WID-SEC-2024-1186
cert-bund:	WID-SEC-2024-0794
cert-bund:	WID-SEC-2023-2031
cert-bund:	WID-SEC-2023-1969
cert-bund:	WID-SEC-2023-1432
cert-bund:	WID-SEC-2022-1777
cert-bund:	WID-SEC-2022-1776
cert-bund:	WID-SEC-2022-1461
cert-bund:	WID-SEC-2022-1245
cert-bund:	WID-SEC-2022-1146
cert-bund:	WID-SEC-2022-1068
cert-bund:	WID-SEC-2022-1065
cert-bund:	WID-SEC-2022-0561
dfn-cert:	DFN-CERT-2024-0147
dfn-cert:	DFN-CERT-2023-2667
dfn-cert:	DFN-CERT-2023-2491
dfn-cert:	DFN-CERT-2023-1230
dfn-cert:	DFN-CERT-2023-0299
dfn-cert:	DFN-CERT-2023-0100
dfn-cert:	DFN-CERT-2022-2323
dfn-cert:	DFN-CERT-2022-2315
dfn-cert:	DFN-CERT-2022-2306
dfn-cert:	DFN-CERT-2022-2150
dfn-cert:	DFN-CERT-2022-2073
dfn-cert:	DFN-CERT-2022-2072
dfn-cert:	DFN-CERT-2022-1905
dfn-cert:	DFN-CERT-2022-1646
dfn-cert:	DFN-CERT-2022-1536
dfn-cert:	DFN-CERT-2022-1521
dfn-cert:	DFN-CERT-2022-1520
dfn-cert:	DFN-CERT-2022-1515
dfn-cert:	DFN-CERT-2022-1497

Medium (CVSS: 5.3) NVT: Mozilla Firefox 'HEIST' Vulnerabilities
Product detection result cpe:/a:mozilla:firefox:136.0 Detected by Mozilla Firefox Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.2 ↪5623.1.0.800017)
Summary Mozilla Firefox might be prone to multiple vulnerabilities dubbed 'HEIST'.
Quality of Detection (QoD): 1%
... continues on next page ...

...continued from previous page...
Vulnerability Detection Result Installed version: 136.0 Fixed version: None, see the references for mitigation steps. Installation path / port: /usr/bin/firefox
Solution: Solution type: Mitigation Make sure to disable third-party cookies in the browser. Please see the references for more information.
Affected Software/OS Mozilla Firefox when using a web-browser configuration in which third-party cookies are sent.
Vulnerability Insight HEIST enables an attacker to conduct BREACH attack against HTTP compression and CRIME attack against TLS compression without being in a man-in-the-middle position. HEIST uses a side-channel attack involving TCP-windows to leak the exact size of any cross-origin response, without having to observe traffic at the network level. Thus, HEIST enables compression-based attacks such as CRIME and BREACH to be performed purely in the browser, by any malicious website or script, without requiring a man-in-the-middle position. HEIST stands for 'HTTP Encrypted Information can be Stolen through TCP-windows'.
Vulnerability Detection Method Reports if Mozilla Firefox is installed on the target. Details: Mozilla Firefox 'HEIST' Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.104818 Version used: 2023-06-28T05:05:22Z
Product Detection Result Product: cpe:/a:mozilla:firefox:136.0 Method: Mozilla Firefox Detection (Linux/Unix SSH Login) OID: 1.3.6.1.4.1.25623.1.0.800017)
References cve: CVE-2016-7152 cve: CVE-2016-7153 url: https://www.blackhat.com/docs/us-16/materials/us-16-VanGoethem-HEIST-HTTP-Encrypted-Information-Can-Be-Stolen-Through-TCP-Windows-wp.pdf url: https://bugzilla.redhat.com/show_bug.cgi?id=1388003 url: https://bugzilla.redhat.com/show_bug.cgi?id=1388005 url: https://support.mozilla.org/en-US/kb/third-party-cookies-firefox-tracking-protection

Medium (CVSS: 5.3) NVT: Mozilla Firefox 'HEIST' Vulnerabilities
Product detection result cpe:/a:mozilla:firefox:136.0 Detected by Mozilla Firefox Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.2 ↪5623.1.0.800017)
Summary Mozilla Firefox might be prone to multiple vulnerabilities dubbed 'HEIST'.
Quality of Detection (QoD): 1%
Vulnerability Detection Result Installed version: 136.0 Fixed version: None, see the references for mitigation steps. Installation path / port: /snap/firefox/5836/usr/lib/firefox/firefox
Solution: Solution type: Mitigation Make sure to disable third-party cookies in the browser. Please see the references for more information.
Affected Software/OS Mozilla Firefox when using a web-browser configuration in which third-party cookies are sent.
Vulnerability Insight HEIST enables an attacker to conduct BREACH attack against HTTP compression and CRIME attack against TLS compression without being in a man-in-the-middle position. HEIST uses a side-channel attack involving TCP-windows to leak the exact size of any cross-origin response, without having to observe traffic at the network level. Thus, HEIST enables compression-based attacks such as CRIME and BREACH to be performed purely in the browser, by any malicious website or script, without requiring a man-in-the-middle position. HEIST stands for 'HTTP Encrypted Information can be Stolen through TCP-windows'.
Vulnerability Detection Method Reports if Mozilla Firefox is installed on the target. Details: Mozilla Firefox 'HEIST' Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.104818 Version used: 2023-06-28T05:05:22Z
Product Detection Result Product: cpe:/a:mozilla:firefox:136.0 Method: Mozilla Firefox Detection (Linux/Unix SSH Login)
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.800017)
References cve: CVE-2016-7152 cve: CVE-2016-7153 url: https://www.blackhat.com/docs/us-16/materials/us-16-VanGoethem-HEIST-HTTP-E↵ncrypted-Information-Can-Be-Stolen-Through-TCP-Windows-wp.pdf url: https://bugzilla.redhat.com/show_bug.cgi?id=1388003 url: https://bugzilla.redhat.com/show_bug.cgi?id=1388005 url: https://support.mozilla.org/en-US/kb/third-party-cookies-firefox-tracking-p↵rotection
Medium (CVSS: 5.3) NVT: Mozilla Firefox 'HEIST' Vulnerabilities
Product detection result cpe:/a:mozilla:firefox:136.0 Detected by Mozilla Firefox Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.2↵5623.1.0.800017)
Summary Mozilla Firefox might be prone to multiple vulnerabilities dubbed 'HEIST'.
Quality of Detection (QoD): 1%
Vulnerability Detection Result Installed version: 130.0 Fixed version: None, see the references for mitigation steps. Installation path / port: /snap/firefox/4848/usr/lib/firefox/firefox
Solution: Solution type: Mitigation Make sure to disable third-party cookies in the browser. Please see the references for more information.
Affected Software/OS Mozilla Firefox when using a web-browser configuration in which third-party cookies are sent.
Vulnerability Insight ... continues on next page ...

...continued from previous page...
<p>HEIST enables an attacker to conduct BREACH attack against HTTP compression and CRIME attack against TLS compression without being in a man-in-the-middle position. HEIST uses a side-channel attack involving TCP-windows to leak the exact size of any cross-origin response, without having to observe traffic at the network level. Thus, HEIST enables compression-based attacks such as CRIME and BREACH to be performed purely in the browser, by any malicious website or script, without requiring a man-in-the-middle position.</p> <p>HEIST stands for 'HTTP Encrypted Information can be Stolen through TCP-windows'.</p>
<p>Vulnerability Detection Method Reports if Mozilla Firefox is installed on the target. Details: Mozilla Firefox 'HEIST' Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.104818 Version used: 2023-06-28T05:05:22Z</p>
<p>Product Detection Result Product: cpe:/a:mozilla:firefox:136.0 Method: Mozilla Firefox Detection (Linux/Unix SSH Login) OID: 1.3.6.1.4.1.25623.1.0.800017)</p>
<p>References cve: CVE-2016-7152 cve: CVE-2016-7153 url: https://www.blackhat.com/docs/us-16/materials/us-16-VanGoethem-HEIST-HTTP-Encrypted-Information-Can-Be-Stolen-Through-TCP-Windows-wp.pdf url: https://bugzilla.redhat.com/show_bug.cgi?id=1388003 url: https://bugzilla.redhat.com/show_bug.cgi?id=1388005 url: https://support.mozilla.org/en-US/kb/third-party-cookies-firefox-tracking-protection</p>
<p>Medium (CVSS: 5.3) NVT: OpenSSL DoS Vulnerability (20231106) - Linux</p>
<p>Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
<p>Summary OpenSSL is prone to a denial of service (DoS) vulnerability.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.13 Installation</p>
... continues on next page ...

...continued from previous page...	
path / port:	/snap/core22/1612/usr/bin/openssl
Impact Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a denial of service.	
Solution: Solution type: VendorFix Update to version 1.0.2zj, 1.1.1x, 3.0.13, 3.1.5 or later.	
Affected Software/OS OpenSSL versions 1.0.2, 1.1.1, 3.0 and 3.1.	
Vulnerability Insight Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20231106) - Linux OID: 1.3.6.1.4.1.25623.1.0.170675 Version used: 2024-01-30T14:37:03Z	
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)	
References cve: CVE-2023-5678 url: https://www.openssl.org/news/secadv/20231106.txt cert-bund: WID-SEC-2025-0148 cert-bund: WID-SEC-2024-3377 cert-bund: WID-SEC-2024-2112 cert-bund: WID-SEC-2024-2100 cert-bund: WID-SEC-2024-1653 cert-bund: WID-SEC-2024-1488 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0769 cert-bund: WID-SEC-2023-2838 dfn-cert: DFN-CERT-2024-2884 dfn-cert: DFN-CERT-2024-2795	
... continues on next page ...	

...continued from previous page ...
dfn-cert: DFN-CERT-2024-1413
dfn-cert: DFN-CERT-2024-1166
dfn-cert: DFN-CERT-2024-1067
dfn-cert: DFN-CERT-2024-0764
dfn-cert: DFN-CERT-2024-0732
dfn-cert: DFN-CERT-2024-0723
dfn-cert: DFN-CERT-2024-0722
dfn-cert: DFN-CERT-2024-0531
dfn-cert: DFN-CERT-2024-0374
dfn-cert: DFN-CERT-2024-0296
dfn-cert: DFN-CERT-2024-0253
dfn-cert: DFN-CERT-2024-0191
dfn-cert: DFN-CERT-2023-2960
dfn-cert: DFN-CERT-2023-2740

Medium (CVSS: 5.3) NVT: OpenSSL DoS Vulnerability (20231106) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.13 Installation path / port: /snap/core22/1748/usr/bin/openssl
Impact Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a denial of service.
Solution: Solution type: VendorFix Update to version 1.0.2zj, 1.1.1x, 3.0.13, 3.1.5 or later.
Affected Software/OS OpenSSL versions 1.0.2, 1.1.1, 3.0 and 3.1.
... continues on next page ...

...continued from previous page...

Vulnerability Insight

Applications that use the functions `DH_generate_key()` to generate an X9.42 DH key may experience long delays. Likewise, applications that use `DH_check_pub_key()`, `DH_check_pub_key_ex()` or `EVP_PKEY_public_check()` to check an X9.42 DH key or X9.42 DH parameters may experience long delays.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
 Details: **OpenSSL DoS Vulnerability (20231106) - Linux**
 OID: 1.3.6.1.4.1.25623.1.0.170675
 Version used: 2024-01-30T14:37:03Z

Product Detection Result

Product: `cpe:/a:openssl:openssl:3.0.2`
 Method: **OpenSSL Detection Consolidation**
 OID: 1.3.6.1.4.1.25623.1.0.145462)

References

cve: CVE-2023-5678
 url: <https://www.openssl.org/news/secadv/20231106.txt>
 cert-bund: WID-SEC-2025-0148
 cert-bund: WID-SEC-2024-3377
 cert-bund: WID-SEC-2024-2112
 cert-bund: WID-SEC-2024-2100
 cert-bund: WID-SEC-2024-1653
 cert-bund: WID-SEC-2024-1488
 cert-bund: WID-SEC-2024-1307
 cert-bund: WID-SEC-2024-1226
 cert-bund: WID-SEC-2024-0769
 cert-bund: WID-SEC-2023-2838
 dfn-cert: DFN-CERT-2024-2884
 dfn-cert: DFN-CERT-2024-2795
 dfn-cert: DFN-CERT-2024-1413
 dfn-cert: DFN-CERT-2024-1166
 dfn-cert: DFN-CERT-2024-1067
 dfn-cert: DFN-CERT-2024-0764
 dfn-cert: DFN-CERT-2024-0732
 dfn-cert: DFN-CERT-2024-0723
 dfn-cert: DFN-CERT-2024-0722
 dfn-cert: DFN-CERT-2024-0531
 dfn-cert: DFN-CERT-2024-0374
 dfn-cert: DFN-CERT-2024-0296
 dfn-cert: DFN-CERT-2024-0253
 dfn-cert: DFN-CERT-2024-0191
 dfn-cert: DFN-CERT-2023-2960
 dfn-cert: DFN-CERT-2023-2740

<p>Medium (CVSS: 5.3) NVT: OpenSSL DoS Vulnerability (20231106) - Linux</p>
<p>Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
<p>Summary OpenSSL is prone to a denial of service (DoS) vulnerability.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.13 Installation path / port: /usr/bin/openssl</p>
<p>Impact Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a denial of service.</p>
<p>Solution: Solution type: VendorFix Update to version 1.0.2zj, 1.1.1x, 3.0.13, 3.1.5 or later.</p>
<p>Affected Software/OS OpenSSL versions 1.0.2, 1.1.1, 3.0 and 3.1.</p>
<p>Vulnerability Insight Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20231106) - Linux OID:1.3.6.1.4.1.25623.1.0.170675 Version used: 2024-01-30T14:37:03Z</p>
<p>Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
<p>... continues on next page ...</p>

...continued from previous page ...
References cve: CVE-2023-5678 url: https://www.openssl.org/news/secadv/20231106.txt cert-bund: WID-SEC-2025-0148 cert-bund: WID-SEC-2024-3377 cert-bund: WID-SEC-2024-2112 cert-bund: WID-SEC-2024-2100 cert-bund: WID-SEC-2024-1653 cert-bund: WID-SEC-2024-1488 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0769 cert-bund: WID-SEC-2023-2838 dfn-cert: DFN-CERT-2024-2884 dfn-cert: DFN-CERT-2024-2795 dfn-cert: DFN-CERT-2024-1413 dfn-cert: DFN-CERT-2024-1166 dfn-cert: DFN-CERT-2024-1067 dfn-cert: DFN-CERT-2024-0764 dfn-cert: DFN-CERT-2024-0732 dfn-cert: DFN-CERT-2024-0723 dfn-cert: DFN-CERT-2024-0722 dfn-cert: DFN-CERT-2024-0531 dfn-cert: DFN-CERT-2024-0374 dfn-cert: DFN-CERT-2024-0296 dfn-cert: DFN-CERT-2024-0253 dfn-cert: DFN-CERT-2024-0191 dfn-cert: DFN-CERT-2023-2960 dfn-cert: DFN-CERT-2023-2740

Medium (CVSS: 5.3) NVT: OpenSSL DoS Vulnerability (20230731) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.10
... continues on next page ...

...continued from previous page ...	
Installation	
path / port:	/snap/core22/1612/usr/bin/openssl
Impact	Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service.
Solution:	
Solution type:	VendorFix
	Update to version 1.0.2zi, 1.1.1v, 3.0.10, 3.1.2 or later.
Affected Software/OS	
	OpenSSL version 1.0.2, 1.1.1, 3.0 and 3.1.
Vulnerability Insight	
	Checking excessively long DH keys or parameters may be very slow.
Vulnerability Detection Method	
	Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20230731) - Linux OID:1.3.6.1.4.1.25623.1.0.150799 Version used: 2023-10-26T05:07:17Z
Product Detection Result	
	Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References	
	cve: CVE-2023-3817 url: https://www.openssl.org/news/secadv/20230731.txt url: https://www.openssl.org/news/vulnerabilities-1.0.2.html#CVE-2023-3817 url: https://www.openssl.org/news/vulnerabilities-1.1.1.html#CVE-2023-3817 url: https://www.openssl.org/news/vulnerabilities-3.0.html#CVE-2023-3817 url: https://www.openssl.org/news/vulnerabilities-3.1.html#CVE-2023-3817 cert-bund: WID-SEC-2024-2100 cert-bund: WID-SEC-2024-1657 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-1488 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0123 cert-bund: WID-SEC-2024-0064
... continues on next page ...	

...continued from previous page ...
cert-bund: WID-SEC-2024-0053 cert-bund: WID-SEC-2023-2964 cert-bund: WID-SEC-2023-2690 cert-bund: WID-SEC-2023-1926 dfn-cert: DFN-CERT-2024-1856 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-1166 dfn-cert: DFN-CERT-2024-1067 dfn-cert: DFN-CERT-2024-0764 dfn-cert: DFN-CERT-2024-0191 dfn-cert: DFN-CERT-2024-0147 dfn-cert: DFN-CERT-2024-0133 dfn-cert: DFN-CERT-2023-3071 dfn-cert: DFN-CERT-2023-3070 dfn-cert: DFN-CERT-2023-2960 dfn-cert: DFN-CERT-2023-2941 dfn-cert: DFN-CERT-2023-2643 dfn-cert: DFN-CERT-2023-2624 dfn-cert: DFN-CERT-2023-2615 dfn-cert: DFN-CERT-2023-2536 dfn-cert: DFN-CERT-2023-2116 dfn-cert: DFN-CERT-2023-1897 dfn-cert: DFN-CERT-2023-1856 dfn-cert: DFN-CERT-2023-1769 dfn-cert: DFN-CERT-2023-1748

Medium (CVSS: 5.3) NVT: OpenSSL DoS Vulnerability (20230731) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.10 Installation path / port: /snap/core22/1748/usr/bin/openssl
Impact
... continues on next page ...

...continued from previous page ...
Applications that use the functions <code>DH_check()</code> , <code>DH_check_ex()</code> or <code>EVP_PKEY_param_check()</code> to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service.
Solution: Solution type: VendorFix Update to version 1.0.2zi, 1.1.1v, 3.0.10, 3.1.2 or later.
Affected Software/OS OpenSSL version 1.0.2, 1.1.1, 3.0 and 3.1.
Vulnerability Insight Checking excessively long DH keys or parameters may be very slow.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20230731) - Linux OID: 1.3.6.1.4.1.25623.1.0.150799 Version used: 2023-10-26T05:07:17Z
Product Detection Result Product: <code>cpe:/a:openssl:openssl:3.0.2</code> Method: <code>OpenSSL Detection Consolidation</code> OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2023-3817 url: https://www.openssl.org/news/secadv/20230731.txt url: https://www.openssl.org/news/vulnerabilities-1.0.2.html#CVE-2023-3817 url: https://www.openssl.org/news/vulnerabilities-1.1.1.html#CVE-2023-3817 url: https://www.openssl.org/news/vulnerabilities-3.0.html#CVE-2023-3817 url: https://www.openssl.org/news/vulnerabilities-3.1.html#CVE-2023-3817 cert-bund: WID-SEC-2024-2100 cert-bund: WID-SEC-2024-1657 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-1488 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0123 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2024-0053 cert-bund: WID-SEC-2023-2964 cert-bund: WID-SEC-2023-2690 cert-bund: WID-SEC-2023-1926
... continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2024-1856
dfn-cert: DFN-CERT-2024-1799
dfn-cert: DFN-CERT-2024-1166
dfn-cert: DFN-CERT-2024-1067
dfn-cert: DFN-CERT-2024-0764
dfn-cert: DFN-CERT-2024-0191
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2024-0133
dfn-cert: DFN-CERT-2023-3071
dfn-cert: DFN-CERT-2023-3070
dfn-cert: DFN-CERT-2023-2960
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2643
dfn-cert: DFN-CERT-2023-2624
dfn-cert: DFN-CERT-2023-2615
dfn-cert: DFN-CERT-2023-2536
dfn-cert: DFN-CERT-2023-2116
dfn-cert: DFN-CERT-2023-1897
dfn-cert: DFN-CERT-2023-1856
dfn-cert: DFN-CERT-2023-1769
dfn-cert: DFN-CERT-2023-1748

Medium (CVSS: 5.3) NVT: OpenSSL DoS Vulnerability (20230731) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.10 Installation path / port: /usr/bin/openssl
Impact Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service.
... continues on next page ...

...continued from previous page ...
Solution: Solution type: VendorFix Update to version 1.0.2zi, 1.1.1v, 3.0.10, 3.1.2 or later.
Affected Software/OS OpenSSL version 1.0.2, 1.1.1, 3.0 and 3.1.
Vulnerability Insight Checking excessively long DH keys or parameters may be very slow.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20230731) - Linux OID:1.3.6.1.4.1.25623.1.0.150799 Version used: 2023-10-26T05:07:17Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2023-3817 url: https://www.openssl.org/news/secadv/20230731.txt url: https://www.openssl.org/news/vulnerabilities-1.0.2.html#CVE-2023-3817 url: https://www.openssl.org/news/vulnerabilities-1.1.1.html#CVE-2023-3817 url: https://www.openssl.org/news/vulnerabilities-3.0.html#CVE-2023-3817 url: https://www.openssl.org/news/vulnerabilities-3.1.html#CVE-2023-3817 cert-bund: WID-SEC-2024-2100 cert-bund: WID-SEC-2024-1657 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-1488 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0123 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2024-0053 cert-bund: WID-SEC-2023-2964 cert-bund: WID-SEC-2023-2690 cert-bund: WID-SEC-2023-1926 dfn-cert: DFN-CERT-2024-1856 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-1166 dfn-cert: DFN-CERT-2024-1067
... continues on next page ...

...continued from previous page ...

```

dfn-cert: DFN-CERT-2024-0764
dfn-cert: DFN-CERT-2024-0191
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2024-0133
dfn-cert: DFN-CERT-2023-3071
dfn-cert: DFN-CERT-2023-3070
dfn-cert: DFN-CERT-2023-2960
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2643
dfn-cert: DFN-CERT-2023-2624
dfn-cert: DFN-CERT-2023-2615
dfn-cert: DFN-CERT-2023-2536
dfn-cert: DFN-CERT-2023-2116
dfn-cert: DFN-CERT-2023-1897
dfn-cert: DFN-CERT-2023-1856
dfn-cert: DFN-CERT-2023-1769
dfn-cert: DFN-CERT-2023-1748

```

Medium (CVSS: 5.3)

NVT: OpenSSL DoS Vulnerability (20230719) - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

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

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 3.0.2

Fixed version: 3.0.10

Installation

path / port: /snap/core22/1612/usr/bin/openssl

Impact

Applications that use the functions `DH_check()`, `DH_check_ex()` or `EVP_PKEY_param_check()` to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service.

Solution:**Solution type:** VendorFix

Update to version 1.0.2zi, 1.1.1v, 3.0.10, 3.1.2 or later.

... continues on next page ...

...continued from previous page ...
Affected Software/OS OpenSSL version 1.0.2, 1.1.1, 3.0 and 3.1.
Vulnerability Insight Checking excessively long DH keys or parameters may be very slow.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20230719) - Linux OID:1.3.6.1.4.1.25623.1.0.104867 Version used: 2023-10-26T05:07:17Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2023-3446 url: https://www.openssl.org/news/secadv/20230719.txt url: https://www.openssl.org/news/vulnerabilities-1.0.2.html#CVE-2023-3446 url: https://www.openssl.org/news/vulnerabilities-1.1.1.html#CVE-2023-3446 url: https://www.openssl.org/news/vulnerabilities-3.0.html#CVE-2023-3446 url: https://www.openssl.org/news/vulnerabilities-3.1.html#CVE-2023-3446 cert-bund: WID-SEC-2024-2100 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-1488 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2024-0053 cert-bund: WID-SEC-2023-2964 cert-bund: WID-SEC-2023-1833 dfn-cert: DFN-CERT-2024-2451 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-1166 dfn-cert: DFN-CERT-2024-1157 dfn-cert: DFN-CERT-2024-0764 dfn-cert: DFN-CERT-2024-0746 dfn-cert: DFN-CERT-2024-0224 dfn-cert: DFN-CERT-2024-0191 dfn-cert: DFN-CERT-2024-0147 dfn-cert: DFN-CERT-2023-3071 dfn-cert: DFN-CERT-2023-3070
... continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2023-2960
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2643
dfn-cert: DFN-CERT-2023-2615
dfn-cert: DFN-CERT-2023-2116
dfn-cert: DFN-CERT-2023-1897
dfn-cert: DFN-CERT-2023-1856
dfn-cert: DFN-CERT-2023-1769
dfn-cert: DFN-CERT-2023-1760
dfn-cert: DFN-CERT-2023-1738
dfn-cert: DFN-CERT-2023-1661
```

Medium (CVSS: 5.3)

NVT: OpenSSL DoS Vulnerability (20230719) - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

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

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 3.0.2

Fixed version: 3.0.10

Installation

path / port: /snap/core22/1748/usr/bin/openssl

Impact

Applications that use the functions `DH_check()`, `DH_check_ex()` or `EVP_PKEY_param_check()` to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service.

Solution:**Solution type:** VendorFix

Update to version 1.0.2zi, 1.1.1v, 3.0.10, 3.1.2 or later.

Affected Software/OS

OpenSSL version 1.0.2, 1.1.1, 3.0 and 3.1.

Vulnerability Insight

... continues on next page ...

...continued from previous page ...
Checking excessively long DH keys or parameters may be very slow.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20230719) - Linux OID:1.3.6.1.4.1.25623.1.0.104867 Version used: 2023-10-26T05:07:17Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2023-3446 url: https://www.openssl.org/news/secadv/20230719.txt url: https://www.openssl.org/news/vulnerabilities-1.0.2.html#CVE-2023-3446 url: https://www.openssl.org/news/vulnerabilities-1.1.1.html#CVE-2023-3446 url: https://www.openssl.org/news/vulnerabilities-3.0.html#CVE-2023-3446 url: https://www.openssl.org/news/vulnerabilities-3.1.html#CVE-2023-3446 cert-bund: WID-SEC-2024-2100 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-1488 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2024-0053 cert-bund: WID-SEC-2023-2964 cert-bund: WID-SEC-2023-1833 dfn-cert: DFN-CERT-2024-2451 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-1166 dfn-cert: DFN-CERT-2024-1157 dfn-cert: DFN-CERT-2024-0764 dfn-cert: DFN-CERT-2024-0746 dfn-cert: DFN-CERT-2024-0224 dfn-cert: DFN-CERT-2024-0191 dfn-cert: DFN-CERT-2024-0147 dfn-cert: DFN-CERT-2023-3071 dfn-cert: DFN-CERT-2023-3070 dfn-cert: DFN-CERT-2023-2960 dfn-cert: DFN-CERT-2023-2941 dfn-cert: DFN-CERT-2023-2643 dfn-cert: DFN-CERT-2023-2615 dfn-cert: DFN-CERT-2023-2116 dfn-cert: DFN-CERT-2023-1897
...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2023-1856 dfn-cert: DFN-CERT-2023-1769 dfn-cert: DFN-CERT-2023-1760 dfn-cert: DFN-CERT-2023-1738 dfn-cert: DFN-CERT-2023-1661
Medium (CVSS: 5.3) NVT: OpenSSL DoS Vulnerability (20230719) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.10 Installation path / port: /usr/bin/openssl
Impact Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service.
Solution: Solution type: VendorFix Update to version 1.0.2zi, 1.1.1v, 3.0.10, 3.1.2 or later.
Affected Software/OS OpenSSL version 1.0.2, 1.1.1, 3.0 and 3.1.
Vulnerability Insight Checking excessively long DH keys or parameters may be very slow.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20230719) - Linux OID:1.3.6.1.4.1.25623.1.0.104867
... continues on next page ...

...continued from previous page ...
Version used: 2023-10-26T05:07:17Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2023-3446 url: https://www.openssl.org/news/secadv/20230719.txt url: https://www.openssl.org/news/vulnerabilities-1.0.2.html#CVE-2023-3446 url: https://www.openssl.org/news/vulnerabilities-1.1.1.html#CVE-2023-3446 url: https://www.openssl.org/news/vulnerabilities-3.0.html#CVE-2023-3446 url: https://www.openssl.org/news/vulnerabilities-3.1.html#CVE-2023-3446 cert-bund: WID-SEC-2024-2100 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-1488 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2024-0053 cert-bund: WID-SEC-2023-2964 cert-bund: WID-SEC-2023-1833 dfn-cert: DFN-CERT-2024-2451 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-1166 dfn-cert: DFN-CERT-2024-1157 dfn-cert: DFN-CERT-2024-0764 dfn-cert: DFN-CERT-2024-0746 dfn-cert: DFN-CERT-2024-0224 dfn-cert: DFN-CERT-2024-0191 dfn-cert: DFN-CERT-2024-0147 dfn-cert: DFN-CERT-2023-3071 dfn-cert: DFN-CERT-2023-3070 dfn-cert: DFN-CERT-2023-2960 dfn-cert: DFN-CERT-2023-2941 dfn-cert: DFN-CERT-2023-2643 dfn-cert: DFN-CERT-2023-2615 dfn-cert: DFN-CERT-2023-2116 dfn-cert: DFN-CERT-2023-1897 dfn-cert: DFN-CERT-2023-1856 dfn-cert: DFN-CERT-2023-1769 dfn-cert: DFN-CERT-2023-1760 dfn-cert: DFN-CERT-2023-1738 dfn-cert: DFN-CERT-2023-1661

<p>Medium (CVSS: 5.3) NVT: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)</p>
<p>Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>Summary OpenBSD OpenSSH is prone to an information disclosure vulnerability.</p>
<p>Quality of Detection (QoD): 50%</p>
<p>Vulnerability Detection Result Installed version: 8.9p1 Fixed version: None Installation path / port: /usr/sbin/sshd</p>
<p>Solution: Solution type: WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.</p>
<p>Affected Software/OS All currently OpenSSH versions are known to be affected.</p>
<p>Vulnerability Insight OpenSSH allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012) OID:1.3.6.1.4.1.25623.1.0.117777 Version used: 2022-11-24T10:18:54Z</p>
<p>Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>References cve: CVE-2016-20012</p>
<p>... continues on next page ...</p>

...continued from previous page ...
url: https://github.com/openssh/openssh-portable/pull/270 url: https://rushter.com/blog/public-ssh-keys/ url: https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2024-0229 cert-bund: CB-K21/0979 dfn-cert: DFN-CERT-2024-1260

Medium (CVSS: 5.3) NVT: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 50%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: None Installation path / port: /usr/bin/ssh
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 All currently OpenSSH versions are known to be affected.
Vulnerability Insight OpenSSH allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012) OID:1.3.6.1.4.1.25623.1.0.117777
... continues on next page ...

...continued from previous page ...
Version used: 2022-11-24T10:18:54Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2016-20012 url: https://github.com/openssh/openssh-portable/pull/270 url: https://rushter.com/blog/public-ssh-keys/ url: https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2024-0229 cert-bund: CB-K21/0979 dfn-cert: DFN-CERT-2024-1260

Medium (CVSS: 5.3) NVT: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 50%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: None Installation path / port: /snap/core22/1748/usr/sbin/sshd
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 All currently OpenSSH versions are known to be affected.
... continues on next page ...

...continued from previous page ...
Vulnerability Insight OpenSSH allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012) OID:1.3.6.1.4.1.25623.1.0.117777 Version used: 2022-11-24T10:18:54Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2016-20012 url: https://github.com/openssh/openssh-portable/pull/270 url: https://rushter.com/blog/public-ssh-keys/ url: https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2024-0229 cert-bund: CB-K21/0979 dfn-cert: DFN-CERT-2024-1260
Medium (CVSS: 5.3) NVT: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 50%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: None Installation path / port: /snap/core22/1748/usr/bin/ssh
... continues on next page ...

...continued from previous page ...
<p>Solution: Solution type: WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.</p>
<p>Affected Software/OS All currently OpenSSH versions are known to be affected.</p>
<p>Vulnerability Insight OpenSSH allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012) OID:1.3.6.1.4.1.25623.1.0.117777 Version used: 2022-11-24T10:18:54Z</p>
<p>Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>References cve: CVE-2016-20012 url: https://github.com/openssh/openssh-portable/pull/270 url: https://rushter.com/blog/public-ssh-keys/ url: https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2024-0229 cert-bund: CB-K21/0979 dfn-cert: DFN-CERT-2024-1260</p>
Medium (CVSS: 5.3) NVT: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)
<p>Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>Summary ... continues on next page ...</p>

...continued from previous page ...
OpenBSD OpenSSH is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 50%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: None Installation path / port: /snap/core22/1612/usr/sbin/sshd
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 All currently OpenSSH versions are known to be affected.
Vulnerability Insight OpenSSH allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012) OID:1.3.6.1.4.1.25623.1.0.117777 Version used: 2022-11-24T10:18:54Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2016-20012 url: https://github.com/openssh/openssh-portable/pull/270 url: https://rushter.com/blog/public-ssh-keys/ url: https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2024-0229 cert-bund: CB-K21/0979 dfn-cert: DFN-CERT-2024-1260

<p>Medium (CVSS: 5.3) NVT: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)</p>
<p>Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>Summary OpenBSD OpenSSH is prone to an information disclosure vulnerability.</p>
<p>Quality of Detection (QoD): 50%</p>
<p>Vulnerability Detection Result Installed version: 8.9p1 Fixed version: None Installation path / port: /snap/core22/1612/usr/bin/ssh</p>
<p>Solution: Solution type: WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.</p>
<p>Affected Software/OS All currently OpenSSH versions are known to be affected.</p>
<p>Vulnerability Insight OpenSSH allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012) OID:1.3.6.1.4.1.25623.1.0.117777 Version used: 2022-11-24T10:18:54Z</p>
<p>Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>References cve: CVE-2016-20012</p>
<p>... continues on next page ...</p>

...continued from previous page ...
url: https://github.com/openssh/openssh-portable/pull/270
url: https://rushter.com/blog/public-ssh-keys/
url: https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak
cert-bund: WID-SEC-2024-1082
cert-bund: WID-SEC-2024-0229
cert-bund: CB-K21/0979
dfn-cert: DFN-CERT-2024-1260

Medium (CVSS: 5.3) NVT: OpenSSL Information Disclosure Vulnerability (20230714) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.10 Installation path / port: /usr/bin/openssl
Impact Applications that use the AES-SIV algorithm and want to authenticate empty data entries as associated data can be misled by removing, adding or reordering such empty entries as these are ignored by the OpenSSL implementation. The vendor is currently unaware of any such applications.
Solution: Solution type: VendorFix Update to version 3.0.10, 3.1.2 or later.
Affected Software/OS OpenSSL version 3.0 and 3.1.
Vulnerability Insight The AES-SIV cipher implementation contains a bug that causes it to ignore empty associated data entries which are unauthenticated as a consequence.
Vulnerability Detection Method ... continues on next page ...

...continued from previous page ...
<p>Checks if a vulnerable version is present on the target host. Details: OpenSSL Information Disclosure Vulnerability (20230714) - Linux OID:1.3.6.1.4.1.25623.1.0.104838 Version used: 2023-10-26T05:07:17Z</p>
<p>Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
<p>References cve: CVE-2023-2975 url: https://www.openssl.org/news/secadv/20230714.txt url: https://www.openssl.org/news/vulnerabilities-3.0.html#CVE-2023-2975 url: https://www.openssl.org/news/vulnerabilities-3.1.html#CVE-2023-2975 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2023-1760 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-1166 dfn-cert: DFN-CERT-2024-1067 dfn-cert: DFN-CERT-2024-0191 dfn-cert: DFN-CERT-2023-2941 dfn-cert: DFN-CERT-2023-2615 dfn-cert: DFN-CERT-2023-2116 dfn-cert: DFN-CERT-2023-1856 dfn-cert: DFN-CERT-2023-1769 dfn-cert: DFN-CERT-2023-1738 dfn-cert: DFN-CERT-2023-1617</p>
<p>Medium (CVSS: 5.3) NVT: OpenSSL Information Disclosure Vulnerability (20230714) - Linux</p>
<p>Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
<p>Summary OpenSSL is prone to an information disclosure vulnerability.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result Installed version: 3.0.2</p>
... continues on next page ...

...continued from previous page...	
Fixed version:	3.0.10
Installation path / port:	/snap/core22/1748/usr/bin/openssl
Impact Applications that use the AES-SIV algorithm and want to authenticate empty data entries as associated data can be misled by removing, adding or reordering such empty entries as these are ignored by the OpenSSL implementation. The vendor is currently unaware of any such applications.	
Solution: Solution type: VendorFix Update to version 3.0.10, 3.1.2 or later.	
Affected Software/OS OpenSSL version 3.0 and 3.1.	
Vulnerability Insight The AES-SIV cipher implementation contains a bug that causes it to ignore empty associated data entries which are unauthenticated as a consequence.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL Information Disclosure Vulnerability (20230714) - Linux OID:1.3.6.1.4.1.25623.1.0.104838 Version used: 2023-10-26T05:07:17Z	
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)	
References cve: CVE-2023-2975 url: https://www.openssl.org/news/secadv/20230714.txt url: https://www.openssl.org/news/vulnerabilities-3.0.html#CVE-2023-2975 url: https://www.openssl.org/news/vulnerabilities-3.1.html#CVE-2023-2975 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2023-1760 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-1166 dfn-cert: DFN-CERT-2024-1067 dfn-cert: DFN-CERT-2024-0191	
... continues on next page ...	

...continued from previous page ...

```
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2615
dfn-cert: DFN-CERT-2023-2116
dfn-cert: DFN-CERT-2023-1856
dfn-cert: DFN-CERT-2023-1769
dfn-cert: DFN-CERT-2023-1738
dfn-cert: DFN-CERT-2023-1617
```

Medium (CVSS: 5.3)

NVT: OpenSSL Information Disclosure Vulnerability (20230714) - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 3.0.2

Fixed version: 3.0.10

Installation

path / port: /snap/core22/1612/usr/bin/openssl

Impact

Applications that use the AES-SIV algorithm and want to authenticate empty data entries as associated data can be misled by removing, adding or reordering such empty entries as these are ignored by the OpenSSL implementation. The vendor is currently unaware of any such applications.

Solution:**Solution type:** VendorFix

Update to version 3.0.10, 3.1.2 or later.

Affected Software/OS

OpenSSL version 3.0 and 3.1.

Vulnerability Insight

The AES-SIV cipher implementation contains a bug that causes it to ignore empty associated data entries which are unauthenticated as a consequence.

Vulnerability Detection Method

... continues on next page ...

...continued from previous page ...
<p>Checks if a vulnerable version is present on the target host. Details: OpenSSL Information Disclosure Vulnerability (20230714) - Linux OID:1.3.6.1.4.1.25623.1.0.104838 Version used: 2023-10-26T05:07:17Z</p>
<p>Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
<p>References cve: CVE-2023-2975 url: https://www.openssl.org/news/secadv/20230714.txt url: https://www.openssl.org/news/vulnerabilities-3.0.html#CVE-2023-2975 url: https://www.openssl.org/news/vulnerabilities-3.1.html#CVE-2023-2975 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2023-1760 dfn-cert: DFN-CERT-2024-1799 dfn-cert: DFN-CERT-2024-1166 dfn-cert: DFN-CERT-2024-1067 dfn-cert: DFN-CERT-2024-0191 dfn-cert: DFN-CERT-2023-2941 dfn-cert: DFN-CERT-2023-2615 dfn-cert: DFN-CERT-2023-2116 dfn-cert: DFN-CERT-2023-1856 dfn-cert: DFN-CERT-2023-1769 dfn-cert: DFN-CERT-2023-1738 dfn-cert: DFN-CERT-2023-1617</p>
<p>Medium (CVSS: 5.3) NVT: OpenSSL: AES OCB fails to encrypt some bytes (CVE-2022-2097) - Linux</p>
<p>Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
<p>Summary OpenSSL is prone to an information disclosure vulnerability.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result Installed version: 3.0.2</p>
... continues on next page ...

...continued from previous page ...	
Fixed version:	3.0.5
Installation path / port:	/snap/core22/1612/usr/bin/openssl
Solution: Solution type: VendorFix Update to version 1.1.1q, 3.0.5 or later.	
Affected Software/OS OpenSSL version 1.1.1 and 3.0.	
Vulnerability Insight AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of 'in place' encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL: AES OCB fails to encrypt some bytes (CVE-2022-2097) - Linux OID:1.3.6.1.4.1.25623.1.0.148392 Version used: 2022-08-29T10:21:34Z	
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)	
References cve: CVE-2022-2097 url: https://www.openssl.org/news/secadv/20220705.txt cert-bund: WID-SEC-2024-1186 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2023-2031 cert-bund: WID-SEC-2023-1969 cert-bund: WID-SEC-2023-1432 cert-bund: WID-SEC-2022-1777 cert-bund: WID-SEC-2022-1776 cert-bund: WID-SEC-2022-1461 cert-bund: WID-SEC-2022-1245 cert-bund: WID-SEC-2022-1146 cert-bund: WID-SEC-2022-1068 cert-bund: WID-SEC-2022-1065	
... continues on next page ...	

...continued from previous page ...
cert-bund: WID-SEC-2022-0561
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2023-2667
dfn-cert: DFN-CERT-2023-2491
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-0299
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2315
dfn-cert: DFN-CERT-2022-2306
dfn-cert: DFN-CERT-2022-2150
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-1905
dfn-cert: DFN-CERT-2022-1646
dfn-cert: DFN-CERT-2022-1536
dfn-cert: DFN-CERT-2022-1521
dfn-cert: DFN-CERT-2022-1520
dfn-cert: DFN-CERT-2022-1515
dfn-cert: DFN-CERT-2022-1497

Medium (CVSS: 5.3) NVT: PHP < 7.3.26, 7.4.x < 7.4.14, 8.0.x < 8.0.1 Filter Vulnerability (Jan 2021) - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to a vulnerability where FILTER_VALIDATE_URL accepts URLs with invalid userinfo.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.3.26 Installation path / port: /usr/bin/php7.2
Solution: Solution type: VendorFix Update to version 7.3.26, 7.4.14, 8.0.1 or later.
Affected Software/OS
... continues on next page ...

...continued from previous page...
PHP versions prior to 7.3.26, 7.4.x prior to 7.4.14 and 8.0.x prior to 8.0.1.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.3.26, 7.4.x < 7.4.14, 8.0.x < 8.0.1 Filter Vulnerability (Jan 2021) - L. ↪.. OID:1.3.6.1.4.1.25623.1.0.145114 Version used: 2021-11-29T15:00:35Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2020-7071 url: https://www.php.net/ChangeLog-7.php#7.3.26 url: https://www.php.net/ChangeLog-7.php#7.4.14 url: https://www.php.net/ChangeLog-8.php#8.0.1 cert-bund: WID-SEC-2023-1737 cert-bund: WID-SEC-2022-2114 cert-bund: CB-K21/0009 dfn-cert: DFN-CERT-2024-2707 dfn-cert: DFN-CERT-2024-1586 dfn-cert: DFN-CERT-2023-1600 dfn-cert: DFN-CERT-2022-2639 dfn-cert: DFN-CERT-2022-2638 dfn-cert: DFN-CERT-2021-2373 dfn-cert: DFN-CERT-2021-1645 dfn-cert: DFN-CERT-2021-1509 dfn-cert: DFN-CERT-2021-1453 dfn-cert: DFN-CERT-2021-0380 dfn-cert: DFN-CERT-2021-0013
Medium (CVSS: 5.3) NVT: PHP < 7.3.33, 7.4.x < 7.4.26, 8.0.x < 8.0.13 Security Update (Nov 2021) - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP released new versions which include a security fix.
... continues on next page ...

...continued from previous page ...	
Quality of Detection (QoD): 30%	
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.3.33 Installation path / port: /usr/bin/php7.2	
Solution: Solution type: VendorFix Update to version 7.3.33, 7.4.26, 8.0.13 or later.	
Affected Software/OS PHP prior to version 7.3.33 and version 7.4.x through 7.4.25 and 8.0.x through 8.0.12.	
Vulnerability Insight Fixed bug #79971 (special character is breaking the path in xml function).	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.3.33, 7.4.x < 7.4.26, 8.0.x < 8.0.13 Security Update (Nov 2021) - Linux OID:1.3.6.1.4.1.25623.1.0.147187 Version used: 2021-12-02T03:03:37Z	
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)	
References cve: CVE-2021-21707 url: https://www.php.net/ChangeLog-7.php#7.3.33 url: https://www.php.net/ChangeLog-7.php#7.4.26 url: https://www.php.net/ChangeLog-8.php#8.0.13 url: http://bugs.php.net/79971 cert-bund: WID-SEC-2023-1737 cert-bund: WID-SEC-2022-1767 cert-bund: WID-SEC-2022-0587 cert-bund: WID-SEC-2022-0432 cert-bund: WID-SEC-2022-0302 cert-bund: CB-K21/1213 dfn-cert: DFN-CERT-2023-1600 dfn-cert: DFN-CERT-2022-2869 dfn-cert: DFN-CERT-2022-2639 dfn-cert: DFN-CERT-2022-2638	
... continues on next page ...	

...continued from previous page ...
dfn-cert: DFN-CERT-2022-2598
dfn-cert: DFN-CERT-2022-2499
dfn-cert: DFN-CERT-2022-1516
dfn-cert: DFN-CERT-2022-1493
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0485
dfn-cert: DFN-CERT-2022-0455
dfn-cert: DFN-CERT-2022-0431
dfn-cert: DFN-CERT-2022-0407
dfn-cert: DFN-CERT-2022-0110
dfn-cert: DFN-CERT-2021-2474
dfn-cert: DFN-CERT-2021-2436

Medium (CVSS: 5.3) NVT: OpenSSL: AES OCB fails to encrypt some bytes (CVE-2022-2097) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.5 Installation path / port: /snap/core22/1748/usr/bin/openssl
Solution: Solution type: VendorFix Update to version 1.1.1q, 3.0.5 or later.
Affected Software/OS OpenSSL version 1.1.1 and 3.0.
Vulnerability Insight AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of 'in place' encryption, sixteen bytes of the plaintext would be revealed.
... continues on next page ...

...continued from previous page ...
Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL: AES OCB fails to encrypt some bytes (CVE-2022-2097) - Linux OID:1.3.6.1.4.1.25623.1.0.148392 Version used: 2022-08-29T10:21:34Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2022-2097 url: https://www.openssl.org/news/secadv/20220705.txt cert-bund: WID-SEC-2024-1186 cert-bund: WID-SEC-2024-0794 cert-bund: WID-SEC-2023-2031 cert-bund: WID-SEC-2023-1969 cert-bund: WID-SEC-2023-1432 cert-bund: WID-SEC-2022-1777 cert-bund: WID-SEC-2022-1776 cert-bund: WID-SEC-2022-1461 cert-bund: WID-SEC-2022-1245 cert-bund: WID-SEC-2022-1146 cert-bund: WID-SEC-2022-1068 cert-bund: WID-SEC-2022-1065 cert-bund: WID-SEC-2022-0561 dfn-cert: DFN-CERT-2024-0147 dfn-cert: DFN-CERT-2023-2667 dfn-cert: DFN-CERT-2023-2491 dfn-cert: DFN-CERT-2023-1230 dfn-cert: DFN-CERT-2023-0299 dfn-cert: DFN-CERT-2023-0100 dfn-cert: DFN-CERT-2022-2323 dfn-cert: DFN-CERT-2022-2315 dfn-cert: DFN-CERT-2022-2306 dfn-cert: DFN-CERT-2022-2150 dfn-cert: DFN-CERT-2022-2073 dfn-cert: DFN-CERT-2022-2072 dfn-cert: DFN-CERT-2022-1905 dfn-cert: DFN-CERT-2022-1646 dfn-cert: DFN-CERT-2022-1536 dfn-cert: DFN-CERT-2022-1521
...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2022-1520 dfn-cert: DFN-CERT-2022-1515 dfn-cert: DFN-CERT-2022-1497
Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH < 9.2 Unspecified Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.2 Installation path / port: /snap/core22/1612/usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.2 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.2.
Vulnerability Insight If the CanonicalizeHostname and CanonicalizePermittedCNAMEs options were enabled, and the system/libc resolver did not check that names in DNS responses were valid, then use of these options could allow an attacker with control of DNS to include invalid characters (possibly including wildcards) in names added to known_hosts files when they were updated. These names would still have to match the CanonicalizePermittedCNAMEs allow-list, so practical exploitation appears unlikely.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.2 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104512 Version used: 2025-01-21T05:37:33Z
Product Detection Result ... continues on next page ...

...continued from previous page ...
Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releases/notes.html#9.2 url: https://www.openwall.com/lists/oss-security/2023/02/02/3

Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH < 9.3 Unspecified Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.3 Installation path / port: /usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.3 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.3.
Vulnerability Insight ssh(1): Portable OpenSSH provides an implementation of the getrrsetbyname(3) function if the standard library does not provide it, for use by the VerifyHostKeyDNS feature. A specifically crafted DNS response could cause this function to perform an out-of-bounds read of adjacent stack data, but this condition does not appear to be exploitable beyond denial-of-service to the ssh(1) client. The getrrsetbyname(3) replacement is only included if the system's standard library lacks this function and portable OpenSSH was not compiled with the ldns library (-with-ldns). getrrsetbyname(3) is only invoked if using VerifyHostKeyDNS to fetch SSHFP records. This problem was found by the Coverity static analyzer.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.3 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104635 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releases/notes.html#9.3 url: https://www.openwall.com/lists/oss-security/2023/03/15/8

Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH < 9.2 Unspecified Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.2 Installation path / port: /snap/core22/1612/usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.2 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.2.
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
<p>If the CanonicalizeHostname and CanonicalizePermittedCNAMEs options were enabled, and the system/libc resolver did not check that names in DNS responses were valid, then use of these options could allow an attacker with control of DNS to include invalid characters (possibly including wildcards) in names added to known_hosts files when they were updated. These names would still have to match the CanonicalizePermittedCNAMEs allow-list, so practical exploitation appears unlikely.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.2 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104512 Version used: 2025-01-21T05:37:33Z</p>
<p>Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>References url: https://www.openssh.com/releasenotes.html#9.2 url: https://www.openwall.com/lists/oss-security/2023/02/02/3</p>

<p>Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH < 9.2 Unspecified Vulnerability</p>
<p>Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.2 Installation path / port: /snap/core22/1748/usr/bin/ssh</p>
<p>Solution: Solution type: VendorFix Update to version 9.2 or later.</p>
... continues on next page ...

...continued from previous page ...

Affected Software/OS

OpenBSD OpenSSH prior to version 9.2.

Vulnerability Insight

If the CanonicalizeHostname and CanonicalizePermittedCNAMEs options were enabled, and the system/libc resolver did not check that names in DNS responses were valid, then use of these options could allow an attacker with control of DNS to include invalid characters (possibly including wildcards) in names added to known_hosts files when they were updated. These names would still have to match the CanonicalizePermittedCNAMEs allow-list, so practical exploitation appears unlikely.

Vulnerability Detection Method

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

Details: OpenBSD OpenSSH < 9.2 Unspecified Vulnerability

OID:1.3.6.1.4.1.25623.1.0.104512

Version used: 2025-01-21T05:37:33Z

Product Detection Result

Product: cpe:/a:openbsd:openssh:8.9p1

Method: OpenSSH Detection Consolidation

OID: 1.3.6.1.4.1.25623.1.0.108577)

Referencesurl: <https://www.openssh.com/releasenotes.html#9.2>url: <https://www.openwall.com/lists/oss-security/2023/02/02/3>

Medium (CVSS: 5.0)

NVT: OpenSSL UAF Vulnerability (20240528) - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to a use after free (UAF) vulnerability.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 3.0.2

Fixed version: 3.0.14

Installation

path / port: /snap/core22/1612/usr/bin/openssl

... continues on next page ...

...continued from previous page ...

Impact

A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code.

Solution:

Solution type: VendorFix

Update to version 1.1.1y, 3.0.14, 3.1.6, 3.2.2, 3.3.1 or later.

Affected Software/OS

OpenSSL versions 1.1.1, 3.0, 3.1, 3.2 and 3.3.

Vulnerability Insight

Calling the OpenSSL API function `SSL_free_buffers` may cause memory to be accessed that was previously freed in some situations.

Vulnerability Detection Method

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

Details: [OpenSSL UAF Vulnerability \(20240528\) - Linux](#)

OID:1.3.6.1.4.1.25623.1.0.114640

Version used: 2024-06-13T05:05:46Z

Product Detection Result

Product: `cpe:/a:openssl:openssl:3.0.2`

Method: OpenSSL Detection Consolidation

OID: 1.3.6.1.4.1.25623.1.0.145462)

References

cve: CVE-2024-4741

url: <https://www.openssl.org/news/secadv/20240528.txt>

url: <https://www.openssl.org/news/vulnerabilities.html>

cert-bund: WID-SEC-2025-0225

cert-bund: WID-SEC-2024-3199

cert-bund: WID-SEC-2024-2112

cert-bund: WID-SEC-2024-1240

dfn-cert: DFN-CERT-2024-2884

dfn-cert: DFN-CERT-2024-2736

dfn-cert: DFN-CERT-2024-2681

dfn-cert: DFN-CERT-2024-2191

dfn-cert: DFN-CERT-2024-1978

dfn-cert: DFN-CERT-2024-1968

dfn-cert: DFN-CERT-2024-1904

dfn-cert: DFN-CERT-2024-1587

dfn-cert: DFN-CERT-2024-1423

Medium (CVSS: 5.0) NVT: OpenSSL UAF Vulnerability (20240528) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a use after free (UAF) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.14 Installation path / port: /snap/core22/1748/usr/bin/openssl
Impact A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code.
Solution: Solution type: VendorFix Update to version 1.1.1y, 3.0.14, 3.1.6, 3.2.2, 3.3.1 or later.
Affected Software/OS OpenSSL versions 1.1.1, 3.0, 3.1, 3.2 and 3.3.
Vulnerability Insight Calling the OpenSSL API function SSL_free_buffers may cause memory to be accessed that was previously freed in some situations.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL UAF Vulnerability (20240528) - Linux OID:1.3.6.1.4.1.25623.1.0.114640 Version used: 2024-06-13T05:05:46Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References ... continues on next page ...

...continued from previous page ...
cve: CVE-2024-4741 url: https://www.openssl.org/news/secadv/20240528.txt url: https://www.openssl.org/news/vulnerabilities.html cert-bund: WID-SEC-2025-0225 cert-bund: WID-SEC-2024-3199 cert-bund: WID-SEC-2024-2112 cert-bund: WID-SEC-2024-1240 dfn-cert: DFN-CERT-2024-2884 dfn-cert: DFN-CERT-2024-2736 dfn-cert: DFN-CERT-2024-2681 dfn-cert: DFN-CERT-2024-2191 dfn-cert: DFN-CERT-2024-1978 dfn-cert: DFN-CERT-2024-1968 dfn-cert: DFN-CERT-2024-1904 dfn-cert: DFN-CERT-2024-1587 dfn-cert: DFN-CERT-2024-1423

Medium (CVSS: 5.0) NVT: OpenSSL UAF Vulnerability (20240528) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a use after free (UAF) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.14 Installation path / port: /usr/bin/openssl
Impact A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code.
Solution: Solution type: VendorFix Update to version 1.1.1y, 3.0.14, 3.1.6, 3.2.2, 3.3.1 or later.
Affected Software/OS ... continues on next page ...

...continued from previous page ...
OpenSSL versions 1.1.1, 3.0, 3.1, 3.2 and 3.3.
Vulnerability Insight Calling the OpenSSL API function SSL_free_buffers may cause memory to be accessed that was previously freed in some situations.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL UAF Vulnerability (20240528) - Linux OID:1.3.6.1.4.1.25623.1.0.114640 Version used: 2024-06-13T05:05:46Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2024-4741 url: https://www.openssl.org/news/secadv/20240528.txt url: https://www.openssl.org/news/vulnerabilities.html cert-bund: WID-SEC-2025-0225 cert-bund: WID-SEC-2024-3199 cert-bund: WID-SEC-2024-2112 cert-bund: WID-SEC-2024-1240 dfn-cert: DFN-CERT-2024-2884 dfn-cert: DFN-CERT-2024-2736 dfn-cert: DFN-CERT-2024-2681 dfn-cert: DFN-CERT-2024-2191 dfn-cert: DFN-CERT-2024-1978 dfn-cert: DFN-CERT-2024-1968 dfn-cert: DFN-CERT-2024-1904 dfn-cert: DFN-CERT-2024-1587 dfn-cert: DFN-CERT-2024-1423
Medium (CVSS: 5.0) NVT: OpenSSL Timing Side-Channel Vulnerability (20250120) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a timing side-channel vulnerability.
... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.16 Installation path / port: /snap/core22/1612/usr/bin/openssl
Impact A timing side-channel in ECDSA signature computations could allow recovering the private key by an attacker. However, measuring the timing would require either local access to the signing application or a very fast network connection with low latency. There is a timing signal of around 300 nanoseconds when the top word of the inverted ECDSA nonce value is zero. This can happen with significant probability only for some of the supported elliptic curves. In particular the NIST P-521 curve is affected. To be able to measure this leak, the attacker process must either be located in the same physical computer or must have a very fast network connection with low latency. For that reason the severity of this vulnerability is Low.
Solution: Solution type: VendorFix Update to version 1.0.2zl, 1.1.1zb, 3.0.16, 3.1.8, 3.2.4, 3.3.3, 3.4.1 or later once available. Note: As of 01/2025 these updates have not been released yet.
Affected Software/OS OpenSSL versions 1.0.2, 1.1.1, 3.0, 3.1, 3.2, 3.3 and 3.4.
Vulnerability Insight A timing side-channel which could potentially allow recovering the private key exists in the ECDSA signature computation.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL Timing Side-Channel Vulnerability (20250120) - Linux OID: 1.3.6.1.4.1.25623.1.0.114924 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2024-13176
... continues on next page ...

...continued from previous page ...
url: https://openssl-library.org/news/secadv/20250120.txt url: https://openssl-library.org/news/vulnerabilities/ cert-bund: WID-SEC-2025-0131 dfn-cert: DFN-CERT-2025-0158
Medium (CVSS: 5.0) NVT: OpenSSL Timing Side-Channel Vulnerability (20250120) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a timing side-channel vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.16 Installation path / port: /snap/core22/1748/usr/bin/openssl
Impact A timing side-channel in ECDSA signature computations could allow recovering the private key by an attacker. However, measuring the timing would require either local access to the signing application or a very fast network connection with low latency. There is a timing signal of around 300 nanoseconds when the top word of the inverted ECDSA nonce value is zero. This can happen with significant probability only for some of the supported elliptic curves. In particular the NIST P-521 curve is affected. To be able to measure this leak, the attacker process must either be located in the same physical computer or must have a very fast network connection with low latency. For that reason the severity of this vulnerability is Low.
Solution: Solution type: VendorFix Update to version 1.0.2zl, 1.1.1zb, 3.0.16, 3.1.8, 3.2.4, 3.3.3, 3.4.1 or later once available. Note: As of 01/2025 these updates have not been released yet.
Affected Software/OS OpenSSL versions 1.0.2, 1.1.1, 3.0, 3.1, 3.2, 3.3 and 3.4.
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
A timing side-channel which could potentially allow recovering the private key exists in the ECDSA signature computation.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL Timing Side-Channel Vulnerability (20250120) - Linux OID:1.3.6.1.4.1.25623.1.0.114924 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2024-13176 url: https://openssl-library.org/news/secadv/20250120.txt url: https://openssl-library.org/news/vulnerabilities/ cert-bund: WID-SEC-2025-0131 dfn-cert: DFN-CERT-2025-0158

Medium (CVSS: 5.0) NVT: OpenSSL Timing Side-Channel Vulnerability (20250120) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a timing side-channel vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.16 Installation path / port: /usr/bin/openssl
Impact A timing side-channel in ECDSA signature computations could allow recovering the private key by an attacker. However, measuring the timing would require either local access to the signing application or a very fast network connection with low latency.
... continues on next page ...

...continued from previous page ...
<p>There is a timing signal of around 300 nanoseconds when the top word of the inverted ECDSA nonce value is zero. This can happen with significant probability only for some of the supported elliptic curves. In particular the NIST P-521 curve is affected. To be able to measure this leak, the attacker process must either be located in the same physical computer or must have a very fast network connection with low latency. For that reason the severity of this vulnerability is Low.</p>
<p>Solution: Solution type: VendorFix Update to version 1.0.2zl, 1.1.1zb, 3.0.16, 3.1.8, 3.2.4, 3.3.3, 3.4.1 or later once available. Note: As of 01/2025 these updates have not been released yet.</p>
<p>Affected Software/OS OpenSSL versions 1.0.2, 1.1.1, 3.0, 3.1, 3.2, 3.3 and 3.4.</p>
<p>Vulnerability Insight A timing side-channel which could potentially allow recovering the private key exists in the ECDSA signature computation.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL Timing Side-Channel Vulnerability (20250120) - Linux OID:1.3.6.1.4.1.25623.1.0.114924 Version used: 2025-01-21T05:37:33Z</p>
<p>Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
<p>References cve: CVE-2024-13176 url: https://openssl-library.org/news/secadv/20250120.txt url: https://openssl-library.org/news/vulnerabilities/ cert-bund: WID-SEC-2025-0131 dfn-cert: DFN-CERT-2025-0158</p>
<p>Medium (CVSS: 5.0) NVT: OpenSSL OOB Memory Access Vulnerability (20241016) - Linux</p>
<p>Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
... continues on next page ...

...continued from previous page ...
Summary OpenSSL is prone to an out of bound (OOB) memory access vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.16 Installation path / port: /snap/core22/1612/usr/bin/openssl
Impact Out of bound memory writes can lead to an application crash or even a possibility of a remote code execution, however, in all the protocols involving Elliptic Curve Cryptography that we're aware of, either only 'named curves' are supported, or, if explicit curve parameters are supported, they specify an X9.62 encoding of binary ($GF(2^m)$) curves that can't represent problematic input values. Thus the likelihood of existence of a vulnerable application is low.
Solution: Solution type: VendorFix Update to version 1.0.2zl, 1.1.1zb, 3.0.16, 3.1.8, 3.2.4, 3.3.3 or later once available. Note: As of 01/2025 these updates have not been released yet.
Affected Software/OS OpenSSL versions 1.0.2, 1.1.1, 3.0, 3.1, 3.2 and 3.3.
Vulnerability Insight Use of the low-level $GF(2^m)$ elliptic curve APIs with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL OOB Memory Access Vulnerability (20241016) - Linux OID:1.3.6.1.4.1.25623.1.0.114828 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2024-9143 url: https://openssl-library.org/news/secadv/20241016.txt
... continues on next page ...

...continued from previous page ...
url: https://openssl-library.org/news/vulnerabilities/ cert-bund: WID-SEC-2025-0148 cert-bund: WID-SEC-2024-3230 dfn-cert: DFN-CERT-2024-2884 dfn-cert: DFN-CERT-2024-2764

Medium (CVSS: 5.0) NVT: OpenSSL DoS Vulnerability (20240408) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.14 Installation path / port: /snap/core22/1748/usr/bin/openssl
Impact An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service.
Solution: Solution type: VendorFix Update to version 1.1.1y, 3.0.14, 3.1.6, 3.2.2 or later.
Affected Software/OS OpenSSL versions 1.1.1, 3.0, 3.1 and 3.2.
Vulnerability Insight Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20240408) - Linux OID:1.3.6.1.4.1.25623.1.0.152058 Version used: 2024-04-10T05:05:22Z
... continues on next page ...

...continued from previous page ...

Product Detection Result

Product: cpe:/a:openssl:openssl:3.0.2
 Method: OpenSSL Detection Consolidation
 OID: 1.3.6.1.4.1.25623.1.0.145462)

References

cve: CVE-2024-2511
 url: <https://www.openssl.org/news/secadv/20240408.txt>
 cert-bund: WID-SEC-2025-0225
 cert-bund: WID-SEC-2024-3192
 cert-bund: WID-SEC-2024-3191
 cert-bund: WID-SEC-2024-2112
 cert-bund: WID-SEC-2024-1638
 cert-bund: WID-SEC-2024-0813
 dfn-cert: DFN-CERT-2024-2884
 dfn-cert: DFN-CERT-2024-2743
 dfn-cert: DFN-CERT-2024-2681
 dfn-cert: DFN-CERT-2024-2191
 dfn-cert: DFN-CERT-2024-2168
 dfn-cert: DFN-CERT-2024-1978
 dfn-cert: DFN-CERT-2024-1904
 dfn-cert: DFN-CERT-2024-1867
 dfn-cert: DFN-CERT-2024-1493
 dfn-cert: DFN-CERT-2024-0916

Medium (CVSS: 5.0)

NVT: OpenSSL OOB Memory Access Vulnerability (20241016) - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2
 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

OpenSSL is prone to an out of bound (OOB) memory access vulnerability.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 3.0.2
 Fixed version: 3.0.16
 Installation
 path / port: /snap/core22/1748/usr/bin/openssl

Impact

... continues on next page ...

...continued from previous page ...
<p>Out of bound memory writes can lead to an application crash or even a possibility of a remote code execution, however, in all the protocols involving Elliptic Curve Cryptography that we're aware of, either only 'named curves' are supported, or, if explicit curve parameters are supported, they specify an X9.62 encoding of binary ($GF(2^m)$) curves that can't represent problematic input values. Thus the likelihood of existence of a vulnerable application is low.</p>
<p>Solution: Solution type: VendorFix Update to version 1.0.2zl, 1.1.1zb, 3.0.16, 3.1.8, 3.2.4, 3.3.3 or later once available. Note: As of 01/2025 these updates have not been released yet.</p>
<p>Affected Software/OS OpenSSL versions 1.0.2, 1.1.1, 3.0, 3.1, 3.2 and 3.3.</p>
<p>Vulnerability Insight Use of the low-level $GF(2^m)$ elliptic curve APIs with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL OOB Memory Access Vulnerability (20241016) - Linux OID:1.3.6.1.4.1.25623.1.0.114828 Version used: 2025-01-21T05:37:33Z</p>
<p>Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
<p>References cve: CVE-2024-9143 url: https://openssl-library.org/news/secadv/20241016.txt url: https://openssl-library.org/news/vulnerabilities/ cert-bund: WID-SEC-2025-0148 cert-bund: WID-SEC-2024-3230 dfn-cert: DFN-CERT-2024-2884 dfn-cert: DFN-CERT-2024-2764</p>
<p>Medium (CVSS: 5.0) NVT: OpenSSL OOB Memory Access Vulnerability (20241016) - Linux</p>
<p>Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
... continues on next page ...

...continued from previous page ...
Summary OpenSSL is prone to an out of bound (OOB) memory access vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.16 Installation path / port: /usr/bin/openssl
Impact Out of bound memory writes can lead to an application crash or even a possibility of a remote code execution, however, in all the protocols involving Elliptic Curve Cryptography that we're aware of, either only 'named curves' are supported, or, if explicit curve parameters are supported, they specify an X9.62 encoding of binary ($GF(2^m)$) curves that can't represent problematic input values. Thus the likelihood of existence of a vulnerable application is low.
Solution: Solution type: VendorFix Update to version 1.0.2zl, 1.1.1zb, 3.0.16, 3.1.8, 3.2.4, 3.3.3 or later once available. Note: As of 01/2025 these updates have not been released yet.
Affected Software/OS OpenSSL versions 1.0.2, 1.1.1, 3.0, 3.1, 3.2 and 3.3.
Vulnerability Insight Use of the low-level $GF(2^m)$ elliptic curve APIs with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL OOB Memory Access Vulnerability (20241016) - Linux OID:1.3.6.1.4.1.25623.1.0.114828 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2024-9143
... continues on next page ...

...continued from previous page ...
url: https://openssl-library.org/news/secadv/20241016.txt
url: https://openssl-library.org/news/vulnerabilities/
cert-bund: WID-SEC-2025-0148
cert-bund: WID-SEC-2024-3230
dfn-cert: DFN-CERT-2024-2884
dfn-cert: DFN-CERT-2024-2764

Medium (CVSS: 5.0) NVT: OpenSSL Buffer Overread Vulnerability (20240627) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a buffer overread vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.15 Installation path / port: /snap/core22/1612/usr/bin/openssl
Impact A buffer overread can have a range of potential consequences such as unexpected application behaviour or a crash.
Solution: Solution type: VendorFix Update to version 1.0.2zk, 1.1.1za, 3.0.15, 3.1.7, 3.2.3, 3.3.2 or later.
Affected Software/OS OpenSSL versions 1.0.2, 1.1.1, 3.0, 3.1, 3.2 and 3.3.
Vulnerability Insight Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL Buffer Overread Vulnerability (20240627) - Linux OID:1.3.6.1.4.1.25623.1.0.114675 ... continues on next page ...

...continued from previous page ...
Version used: 2024-10-18T05:05:38Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2024-5535 url: https://openssl-library.org/news/secadv/20240627.txt url: https://openssl-library.org/news/vulnerabilities/ cert-bund: WID-SEC-2025-0225 cert-bund: WID-SEC-2025-0166 cert-bund: WID-SEC-2025-0148 cert-bund: WID-SEC-2025-0143 cert-bund: WID-SEC-2024-3674 cert-bund: WID-SEC-2024-3412 cert-bund: WID-SEC-2024-3192 cert-bund: WID-SEC-2024-3188 cert-bund: WID-SEC-2024-2112 cert-bund: WID-SEC-2024-1469 dfn-cert: DFN-CERT-2025-0179 dfn-cert: DFN-CERT-2025-0175 dfn-cert: DFN-CERT-2025-0170 dfn-cert: DFN-CERT-2024-3152 dfn-cert: DFN-CERT-2024-3013 dfn-cert: DFN-CERT-2024-2884 dfn-cert: DFN-CERT-2024-2732 dfn-cert: DFN-CERT-2024-2168 dfn-cert: DFN-CERT-2024-1978 dfn-cert: DFN-CERT-2024-1968 dfn-cert: DFN-CERT-2024-1681
Medium (CVSS: 5.0) NVT: OpenSSL Buffer Overread Vulnerability (20240627) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a buffer overread vulnerability.
Quality of Detection (QoD): 30%
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.15 Installation path / port: /snap/core22/1748/usr/bin/openssl
Impact A buffer overread can have a range of potential consequences such as unexpected application behaviour or a crash.
Solution: Solution type: VendorFix Update to version 1.0.2zk, 1.1.1za, 3.0.15, 3.1.7, 3.2.3, 3.3.2 or later.
Affected Software/OS OpenSSL versions 1.0.2, 1.1.1, 3.0, 3.1, 3.2 and 3.3.
Vulnerability Insight Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL Buffer Overread Vulnerability (20240627) - Linux OID:1.3.6.1.4.1.25623.1.0.114675 Version used: 2024-10-18T05:05:38Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2024-5535 url: https://openssl-library.org/news/secadv/20240627.txt url: https://openssl-library.org/news/vulnerabilities/ cert-bund: WID-SEC-2025-0225 cert-bund: WID-SEC-2025-0166 cert-bund: WID-SEC-2025-0148 cert-bund: WID-SEC-2025-0143 cert-bund: WID-SEC-2024-3674 cert-bund: WID-SEC-2024-3412 cert-bund: WID-SEC-2024-3192 cert-bund: WID-SEC-2024-3188
... continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2024-2112
cert-bund: WID-SEC-2024-1469
dfn-cert: DFN-CERT-2025-0179
dfn-cert: DFN-CERT-2025-0175
dfn-cert: DFN-CERT-2025-0170
dfn-cert: DFN-CERT-2024-3152
dfn-cert: DFN-CERT-2024-3013
dfn-cert: DFN-CERT-2024-2884
dfn-cert: DFN-CERT-2024-2732
dfn-cert: DFN-CERT-2024-2168
dfn-cert: DFN-CERT-2024-1978
dfn-cert: DFN-CERT-2024-1968
dfn-cert: DFN-CERT-2024-1681

Medium (CVSS: 5.0) NVT: OpenSSL Buffer Overread Vulnerability (20240627) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a buffer overread vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.15 Installation path / port: /usr/bin/openssl
Impact A buffer overread can have a range of potential consequences such as unexpected application behaviour or a crash.
Solution: Solution type: VendorFix Update to version 1.0.2zk, 1.1.1za, 3.0.15, 3.1.7, 3.2.3, 3.3.2 or later.
Affected Software/OS OpenSSL versions 1.0.2, 1.1.1, 3.0, 3.1, 3.2 and 3.3.
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL Buffer Overread Vulnerability (20240627) - Linux OID:1.3.6.1.4.1.25623.1.0.114675 Version used: 2024-10-18T05:05:38Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2024-5535 url: https://openssl-library.org/news/secadv/20240627.txt url: https://openssl-library.org/news/vulnerabilities/ cert-bund: WID-SEC-2025-0225 cert-bund: WID-SEC-2025-0166 cert-bund: WID-SEC-2025-0148 cert-bund: WID-SEC-2025-0143 cert-bund: WID-SEC-2024-3674 cert-bund: WID-SEC-2024-3412 cert-bund: WID-SEC-2024-3192 cert-bund: WID-SEC-2024-3188 cert-bund: WID-SEC-2024-2112 cert-bund: WID-SEC-2024-1469 dfn-cert: DFN-CERT-2025-0179 dfn-cert: DFN-CERT-2025-0175 dfn-cert: DFN-CERT-2025-0170 dfn-cert: DFN-CERT-2024-3152 dfn-cert: DFN-CERT-2024-3013 dfn-cert: DFN-CERT-2024-2884 dfn-cert: DFN-CERT-2024-2732 dfn-cert: DFN-CERT-2024-2168 dfn-cert: DFN-CERT-2024-1978 dfn-cert: DFN-CERT-2024-1968 dfn-cert: DFN-CERT-2024-1681
Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH 8.7 - 9.1 Unspecified Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
...continues on next page ...

...continued from previous page ...
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.2 Installation path / port: /usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.2 or later.
Affected Software/OS OpenBSD OpenSSH versions starting from 8.7 and prior to 9.2.
Vulnerability Insight The PermitRemoteOpen option would ignore its first argument unless it was one of the special keywords 'any' or 'none', causing the permission list to fail open if only one permission was specified.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH 8.7 - 9.1 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104511 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releasesnotes.html#9.2 url: https://www.openwall.com/lists/oss-security/2023/02/02/3
Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH 8.7 - 9.1 Unspecified Vulnerability
Product detection result ... continues on next page ...

...continued from previous page ...
cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.2 Installation path / port: /usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.2 or later.
Affected Software/OS OpenBSD OpenSSH versions starting from 8.7 and prior to 9.2.
Vulnerability Insight The PermitRemoteOpen option would ignore its first argument unless it was one of the special keywords 'any' or 'none', causing the permission list to fail open if only one permission was specified.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH 8.7 - 9.1 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104511 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releasesnotes.html#9.2 url: https://www.openwall.com/lists/oss-security/2023/02/02/3

Medium (CVSS: 5.0) NVT: OpenSSL DoS Vulnerability (20240408) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.14 Installation path / port: /snap/core22/1612/usr/bin/openssl
Impact An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service.
Solution: Solution type: VendorFix Update to version 1.1.1y, 3.0.14, 3.1.6, 3.2.2 or later.
Affected Software/OS OpenSSL versions 1.1.1, 3.0, 3.1 and 3.2.
Vulnerability Insight Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20240408) - Linux OID:1.3.6.1.4.1.25623.1.0.152058 Version used: 2024-04-10T05:05:22Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References ... continues on next page ...

...continued from previous page ...
cve: CVE-2024-2511 url: https://www.openssl.org/news/secadv/20240408.txt cert-bund: WID-SEC-2025-0225 cert-bund: WID-SEC-2024-3192 cert-bund: WID-SEC-2024-3191 cert-bund: WID-SEC-2024-2112 cert-bund: WID-SEC-2024-1638 cert-bund: WID-SEC-2024-0813 dfn-cert: DFN-CERT-2024-2884 dfn-cert: DFN-CERT-2024-2743 dfn-cert: DFN-CERT-2024-2681 dfn-cert: DFN-CERT-2024-2191 dfn-cert: DFN-CERT-2024-2168 dfn-cert: DFN-CERT-2024-1978 dfn-cert: DFN-CERT-2024-1904 dfn-cert: DFN-CERT-2024-1867 dfn-cert: DFN-CERT-2024-1493 dfn-cert: DFN-CERT-2024-0916

Medium (CVSS: 5.0) NVT: OpenSSL DoS Vulnerability (20240115) - Linux
Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.13 Installation path / port: /usr/bin/openssl
Impact Where the key that is being checked has been obtained from an untrusted source this may lead to a DoS.
Solution: Solution type: VendorFix Update to version 3.0.13, 3.1.5, 3.2.1 or later.
... continues on next page ...

...continued from previous page ...
Affected Software/OS OpenSSL versions 3.0, 3.1 and 3.2.
Vulnerability Insight Applications that use the function EVP_PKEY_public_check() to check RSA public keys may experience long delays.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20240115) - Linux OID:1.3.6.1.4.1.25623.1.0.114276 Version used: 2024-01-30T14:37:03Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2023-6237 url: https://www.openssl.org/news/secadv/20240115.txt cert-bund: WID-SEC-2024-1488 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0769 cert-bund: WID-SEC-2024-0093 dfn-cert: DFN-CERT-2024-2981 dfn-cert: DFN-CERT-2024-1413 dfn-cert: DFN-CERT-2024-1166 dfn-cert: DFN-CERT-2024-1067 dfn-cert: DFN-CERT-2024-0531 dfn-cert: DFN-CERT-2024-0296 dfn-cert: DFN-CERT-2024-0253 dfn-cert: DFN-CERT-2024-0175 dfn-cert: DFN-CERT-2024-0106
Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH < 9.3 Unspecified Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary
... continues on next page ...

...continued from previous page...
OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.3 Installation path / port: /snap/core22/1612/usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.3 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.3.
Vulnerability Insight ssh(1): Portable OpenSSH provides an implementation of the getrrsetbyname(3) function if the standard library does not provide it, for use by the VerifyHostKeyDNS feature. A specifically crafted DNS response could cause this function to perform an out-of-bounds read of adjacent stack data, but this condition does not appear to be exploitable beyond denial-of-service to the ssh(1) client. The getrrsetbyname(3) replacement is only included if the system's standard library lacks this function and portable OpenSSH was not compiled with the ldns library (-with-ldns). getrrsetbyname(3) is only invoked if using VerifyHostKeyDNS to fetch SSHFP records. This problem was found by the Coverity static analyzer.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.3 Unspecified Vulnerability OID: 1.3.6.1.4.1.25623.1.0.104635 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releasenotes.html#9.3 url: https://www.openwall.com/lists/oss-security/2023/03/15/8

Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH < 9.3 Unspecified Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.3 Installation path / port: /snap/core22/1612/usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.3 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.3.
Vulnerability Insight ssh(1): Portable OpenSSH provides an implementation of the getrrsetbyname(3) function if the standard library does not provide it, for use by the VerifyHostKeyDNS feature. A specifically crafted DNS response could cause this function to perform an out-of-bounds read of adjacent stack data, but this condition does not appear to be exploitable beyond denial-of-service to the ssh(1) client. The getrrsetbyname(3) replacement is only included if the system's standard library lacks this function and portable OpenSSH was not compiled with the ldns library (-with-ldns). getrrsetbyname(3) is only invoked if using VerifyHostKeyDNS to fetch SSHFP records. This problem was found by the Coverity static analyzer.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.3 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104635 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releases/notes.html#9.3 url: https://www.openwall.com/lists/oss-security/2023/03/15/8

Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH < 9.3 Unspecified Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.3 Installation path / port: /snap/core22/1748/usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.3 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.3.
Vulnerability Insight ssh(1): Portable OpenSSH provides an implementation of the getrrsetbyname(3) function if the standard library does not provide it, for use by the VerifyHostKeyDNS feature. A specifically crafted DNS response could cause this function to perform an out-of-bounds read of adjacent stack data, but this condition does not appear to be exploitable beyond denial-of-service to the ssh(1) client. The getrrsetbyname(3) replacement is only included if the system's standard library lacks this function and portable OpenSSH was not compiled with the ldns library (-with-ldns). getrrsetbyname(3) is only invoked if using VerifyHostKeyDNS to fetch SSHFP records. This problem was found by the Coverity static analyzer.
Vulnerability Detection Method ... continues on next page ...

...continued from previous page ...
<p>Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.3 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104635 Version used: 2025-01-21T05:37:33Z</p>
<p>Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>References url: https://www.openssh.com/releases/notes.html#9.3 url: https://www.openwall.com/lists/oss-security/2023/03/15/8</p>

<p>Medium (CVSS: 5.0) NVT: OpenSSL DoS Vulnerability (20240516) - Linux</p>
<p>Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
<p>Summary OpenSSL is prone to a denial of service (DoS) vulnerability.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.14 Installation path / port: /usr/bin/openssl</p>
<p>Impact Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service.</p>
<p>Solution: Solution type: VendorFix Update to version 3.0.14, 3.1.6, 3.2.2, 3.3.1 or later.</p>
<p>Affected Software/OS OpenSSL versions 3.0, 3.1, 3.2 and 3.3.</p>
<p>... continues on next page ...</p>

...continued from previous page ...
Vulnerability Insight Checking excessively long DSA keys or parameters may be very slow. Applications that use the functions <code>EVP_PKEY_param_check()</code> or <code>EVP_PKEY_public_check()</code> to check a DSA public key or DSA parameters may experience long delays.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20240516) - Linux OID:1.3.6.1.4.1.25623.1.0.152250 Version used: 2024-06-13T05:05:46Z
Product Detection Result Product: <code>cpe:/a:openssl:openssl:3.0.2</code> Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2024-4603 url: https://www.openssl.org/news/secadv/20240516.txt url: https://www.openssl.org/news/vulnerabilities.html cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-2112 cert-bund: WID-SEC-2024-1645 cert-bund: WID-SEC-2024-1171 dfn-cert: DFN-CERT-2024-2191 dfn-cert: DFN-CERT-2024-1978 dfn-cert: DFN-CERT-2024-1968 dfn-cert: DFN-CERT-2024-1904 dfn-cert: DFN-CERT-2024-1851 dfn-cert: DFN-CERT-2024-1587 dfn-cert: DFN-CERT-2024-1493 dfn-cert: DFN-CERT-2024-1330
Medium (CVSS: 5.0) NVT: OpenSSL DoS Vulnerability (20240516) - Linux
Product detection result <code>cpe:/a:openssl:openssl:3.0.2</code> Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.14 Installation path / port: /snap/core22/1748/usr/bin/openssl
Impact Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service.
Solution: Solution type: VendorFix Update to version 3.0.14, 3.1.6, 3.2.2, 3.3.1 or later.
Affected Software/OS OpenSSL versions 3.0, 3.1, 3.2 and 3.3.
Vulnerability Insight Checking excessively long DSA keys or parameters may be very slow. Applications that use the functions <code>EVP_PKEY_param_check()</code> or <code>EVP_PKEY_public_check()</code> to check a DSA public key or DSA parameters may experience long delays.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20240516) - Linux OID: 1.3.6.1.4.1.25623.1.0.152250 Version used: 2024-06-13T05:05:46Z
Product Detection Result Product: <code>cpe:/a:openssl:openssl:3.0.2</code> Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2024-4603 url: https://www.openssl.org/news/secadv/20240516.txt url: https://www.openssl.org/news/vulnerabilities.html cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-2112 cert-bund: WID-SEC-2024-1645 cert-bund: WID-SEC-2024-1171 dfn-cert: DFN-CERT-2024-2191
... continues on next page ...

...continued from previous page ...

```
dfn-cert: DFN-CERT-2024-1978
dfn-cert: DFN-CERT-2024-1968
dfn-cert: DFN-CERT-2024-1904
dfn-cert: DFN-CERT-2024-1851
dfn-cert: DFN-CERT-2024-1587
dfn-cert: DFN-CERT-2024-1493
dfn-cert: DFN-CERT-2024-1330
```

Medium (CVSS: 5.0)

NVT: OpenSSL DoS Vulnerability (20240115) - Linux

Product detection result

cpe:/a:openssl:openssl:3.0.2

Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary

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

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 3.0.2

Fixed version: 3.0.13

Installation

path / port: /snap/core22/1748/usr/bin/openssl

Impact

Where the key that is being checked has been obtained from an untrusted source this may lead to a DoS.

Solution:**Solution type:** VendorFix

Update to version 3.0.13, 3.1.5, 3.2.1 or later.

Affected Software/OS

OpenSSL versions 3.0, 3.1 and 3.2.

Vulnerability InsightApplications that use the function `EVP_PKEY_public_check()` to check RSA public keys may experience long delays.**Vulnerability Detection Method**

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

Details: OpenSSL DoS Vulnerability (20240115) - Linux

... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.114276 Version used: 2024-01-30T14:37:03Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2023-6237 url: https://www.openssl.org/news/secadv/20240115.txt cert-bund: WID-SEC-2024-1488 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0769 cert-bund: WID-SEC-2024-0093 dfn-cert: DFN-CERT-2024-2981 dfn-cert: DFN-CERT-2024-1413 dfn-cert: DFN-CERT-2024-1166 dfn-cert: DFN-CERT-2024-1067 dfn-cert: DFN-CERT-2024-0531 dfn-cert: DFN-CERT-2024-0296 dfn-cert: DFN-CERT-2024-0253 dfn-cert: DFN-CERT-2024-0175 dfn-cert: DFN-CERT-2024-0106

Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH < 9.3 Unspecified Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.3 Installation path / port: /snap/core22/1748/usr/sbin/sshd
Solution:
... continues on next page ...

...continued from previous page ...
Solution type: VendorFix Update to version 9.3 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.3.
Vulnerability Insight ssh(1): Portable OpenSSH provides an implementation of the getrrsetbyname(3) function if the standard library does not provide it, for use by the VerifyHostKeyDNS feature. A specifically crafted DNS response could cause this function to perform an out-of-bounds read of adjacent stack data, but this condition does not appear to be exploitable beyond denial-of-service to the ssh(1) client. The getrrsetbyname(3) replacement is only included if the system's standard library lacks this function and portable OpenSSH was not compiled with the ldns library (-with-ldns). getrrsetbyname(3) is only invoked if using VerifyHostKeyDNS to fetch SSHFP records. This problem was found by the Coverity static analyzer.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.3 Unspecified Vulnerability OID: 1.3.6.1.4.1.25623.1.0.104635 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releases.html#9.3 url: https://www.openwall.com/lists/oss-security/2023/03/15/8

Medium (CVSS: 5.0) NVT: PHP < 7.3.28, 7.4.x < 7.4.18 IMAP Header Injection Vulnerability (Apr 2021) - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to an IMAP header injection vulnerability.
Quality of Detection (QoD): 30%
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.3.28 Installation path / port: /usr/bin/php7.2
Solution: Solution type: VendorFix Update to version 7.3.28, 7.4.18 or later.
Affected Software/OS PHP versions prior to 7.3.28 and 7.4.x through 7.4.17.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.3.28, 7.4.x < 7.4.18 IMAP Header Injection Vulnerability (Apr 2021) - L. ↪.. OID:1.3.6.1.4.1.25623.1.0.145869 Version used: 2021-05-03T08:21:47Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References url: https://www.php.net/ChangeLog-7.php#7.3.28 url: https://www.php.net/ChangeLog-7.php#7.4.18
Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH < 9.3 Unspecified Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result ... continues on next page ...

...continued from previous page ...	
Installed version:	8.9p1
Fixed version:	9.3
Installation	
path / port:	/usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.3 or later.	
Affected Software/OS OpenBSD OpenSSH prior to version 9.3.	
Vulnerability Insight ssh(1): Portable OpenSSH provides an implementation of the getrrsetbyname(3) function if the standard library does not provide it, for use by the VerifyHostKeyDNS feature. A specifically crafted DNS response could cause this function to perform an out-of-bounds read of adjacent stack data, but this condition does not appear to be exploitable beyond denial-of-service to the ssh(1) client. The getrrsetbyname(3) replacement is only included if the system's standard library lacks this function and portable OpenSSH was not compiled with the ldns library (-with-ldns). getrrsetbyname(3) is only invoked if using VerifyHostKeyDNS to fetch SSHFP records. This problem was found by the Coverity static analyzer.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.3 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104635 Version used: 2025-01-21T05:37:33Z	
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)	
References url: https://www.openssh.com/releases.html#9.3 url: https://www.openwall.com/lists/oss-security/2023/03/15/8	

Medium (CVSS: 5.0)

NVT: PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Aug 2021) - Linux

Product detection result

cpe:/a:php:php:7.2.34

Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

... continues on next page ...

...continued from previous page ...	
Summary PHP released new versions which include security fixes.	
Quality of Detection (QoD): 30%	
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 7.3.30 Installation path / port: /usr/bin/php7.2	
Solution: Solution type: VendorFix Update to version 7.3.30, 7.4.23, 8.0.10 or later.	
Affected Software/OS PHP versions prior to 7.3.30, 7.4.x through 7.4.22 and 8.0.x through 8.0.9.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Aug 2021) - Linux OID:1.3.6.1.4.1.25623.1.0.146584 Version used: 2021-08-27T08:15:01Z	
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)	
References url: https://www.php.net/ChangeLog-7.php#7.3.30 url: https://www.php.net/ChangeLog-7.php#7.4.23 url: https://www.php.net/ChangeLog-8.php#8.0.10	
Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH < 9.2 Unspecified Vulnerability	
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)	
... continues on next page ...	

...continued from previous page ...
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.2 Installation path / port: /snap/core22/1748/usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.2 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.2.
Vulnerability Insight If the CanonicalizeHostname and CanonicalizePermittedCNAMEs options were enabled, and the system/libc resolver did not check that names in DNS responses were valid, then use of these options could allow an attacker with control of DNS to include invalid characters (possibly including wildcards) in names added to known_hosts files when they were updated. These names would still have to match the CanonicalizePermittedCNAMEs allow-list, so practical exploitation appears unlikely.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.2 Unspecified Vulnerability OID: 1.3.6.1.4.1.25623.1.0.104512 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releases/notes.html#9.2 url: https://www.openwall.com/lists/oss-security/2023/02/02/3
Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH < 9.2 Unspecified Vulnerability
... continues on next page ...

...continued from previous page...
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.2 Installation path / port: /usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.2 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.2.
Vulnerability Insight If the CanonicalizeHostname and CanonicalizePermittedCNAMEs options were enabled, and the system/libc resolver did not check that names in DNS responses were valid, then use of these options could allow an attacker with control of DNS to include invalid characters (possibly including wildcards) in names added to known_hosts files when they were updated. These names would still have to match the CanonicalizePermittedCNAMEs allow-list, so practical exploitation appears unlikely.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.2 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104512 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releases.html#9.2 url: https://www.openwall.com/lists/oss-security/2023/02/02/3

<p>Medium (CVSS: 5.0) NVT: OpenSSL DoS Vulnerability (20240516) - Linux</p>
<p>Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
<p>Summary OpenSSL is prone to a denial of service (DoS) vulnerability.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.14 Installation path / port: /snap/core22/1612/usr/bin/openssl</p>
<p>Impact Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service.</p>
<p>Solution: Solution type: VendorFix Update to version 3.0.14, 3.1.6, 3.2.2, 3.3.1 or later.</p>
<p>Affected Software/OS OpenSSL versions 3.0, 3.1, 3.2 and 3.3.</p>
<p>Vulnerability Insight Checking excessively long DSA keys or parameters may be very slow. Applications that use the functions EVP_PKEY_param_check() or EVP_PKEY_public_check() to check a DSA public key or DSA parameters may experience long delays.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20240516) - Linux OID:1.3.6.1.4.1.25623.1.0.152250 Version used: 2024-06-13T05:05:46Z</p>
<p>Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
<p>... continues on next page ...</p>

...continued from previous page ...
References cve: CVE-2024-4603 url: https://www.openssl.org/news/secadv/20240516.txt url: https://www.openssl.org/news/vulnerabilities.html cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-2112 cert-bund: WID-SEC-2024-1645 cert-bund: WID-SEC-2024-1171 dfn-cert: DFN-CERT-2024-2191 dfn-cert: DFN-CERT-2024-1978 dfn-cert: DFN-CERT-2024-1968 dfn-cert: DFN-CERT-2024-1904 dfn-cert: DFN-CERT-2024-1851 dfn-cert: DFN-CERT-2024-1587 dfn-cert: DFN-CERT-2024-1493 dfn-cert: DFN-CERT-2024-1330

Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH < 9.2 Unspecified Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.2 Installation path / port: /usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.2 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.2.
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
<p>If the CanonicalizeHostname and CanonicalizePermittedCNAMEs options were enabled, and the system/libc resolver did not check that names in DNS responses were valid, then use of these options could allow an attacker with control of DNS to include invalid characters (possibly including wildcards) in names added to known_hosts files when they were updated. These names would still have to match the CanonicalizePermittedCNAMEs allow-list, so practical exploitation appears unlikely.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.2 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104512 Version used: 2025-01-21T05:37:33Z</p>
<p>Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>References url: https://www.openssh.com/releases.html#9.2 url: https://www.openwall.com/lists/oss-security/2023/02/02/3</p>

<p>Medium (CVSS: 5.0) NVT: OpenSSL DoS Vulnerability (20240115) - Linux</p>
<p>Product detection result cpe:/a:openssl:openssl:3.0.2 Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)</p>
<p>Summary OpenSSL is prone to a denial of service (DoS) vulnerability.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.13 Installation path / port: /snap/core22/1612/usr/bin/openssl</p>
<p>Impact Where the key that is being checked has been obtained from an untrusted source this may lead to a DoS.</p>
... continues on next page ...

...continued from previous page ...	
Solution: Solution type: VendorFix Update to version 3.0.13, 3.1.5, 3.2.1 or later.	
Affected Software/OS OpenSSL versions 3.0, 3.1 and 3.2.	
Vulnerability Insight Applications that use the function EVP_PKEY_public_check() to check RSA public keys may experience long delays.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20240115) - Linux OID:1.3.6.1.4.1.25623.1.0.114276 Version used: 2024-01-30T14:37:03Z	
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)	
References cve: CVE-2023-6237 url: https://www.openssl.org/news/secadv/20240115.txt cert-bund: WID-SEC-2024-1488 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-0769 cert-bund: WID-SEC-2024-0093 dfn-cert: DFN-CERT-2024-2981 dfn-cert: DFN-CERT-2024-1413 dfn-cert: DFN-CERT-2024-1166 dfn-cert: DFN-CERT-2024-1067 dfn-cert: DFN-CERT-2024-0531 dfn-cert: DFN-CERT-2024-0296 dfn-cert: DFN-CERT-2024-0253 dfn-cert: DFN-CERT-2024-0175 dfn-cert: DFN-CERT-2024-0106	
Medium (CVSS: 5.0) NVT: OpenSSL DoS Vulnerability (20240408) - Linux	
Product detection result cpe:/a:openssl:openssl:3.0.2	
... continues on next page ...	

...continued from previous page ...
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
Summary OpenSSL is prone to a denial of service (DoS) vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.0.2 Fixed version: 3.0.14 Installation path / port: /usr/bin/openssl
Impact An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service.
Solution: Solution type: VendorFix Update to version 1.1.1y, 3.0.14, 3.1.6, 3.2.2 or later.
Affected Software/OS OpenSSL versions 1.1.1, 3.0, 3.1 and 3.2.
Vulnerability Insight Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSL DoS Vulnerability (20240408) - Linux OID:1.3.6.1.4.1.25623.1.0.152058 Version used: 2024-04-10T05:05:22Z
Product Detection Result Product: cpe:/a:openssl:openssl:3.0.2 Method: OpenSSL Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.145462)
References cve: CVE-2024-2511 url: https://www.openssl.org/news/secadv/20240408.txt cert-bund: WID-SEC-2025-0225 cert-bund: WID-SEC-2024-3192
... continues on next page ...

...continued from previous page ...
cert-bund: WID-SEC-2024-3191 cert-bund: WID-SEC-2024-2112 cert-bund: WID-SEC-2024-1638 cert-bund: WID-SEC-2024-0813 dfn-cert: DFN-CERT-2024-2884 dfn-cert: DFN-CERT-2024-2743 dfn-cert: DFN-CERT-2024-2681 dfn-cert: DFN-CERT-2024-2191 dfn-cert: DFN-CERT-2024-2168 dfn-cert: DFN-CERT-2024-1978 dfn-cert: DFN-CERT-2024-1904 dfn-cert: DFN-CERT-2024-1867 dfn-cert: DFN-CERT-2024-1493 dfn-cert: DFN-CERT-2024-0916

Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH 8.7 - 9.1 Unspecified Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.2 Installation path / port: /snap/core22/1612/usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.2 or later.
Affected Software/OS OpenBSD OpenSSH versions starting from 8.7 and prior to 9.2.
Vulnerability Insight The PermitRemoteOpen option would ignore its first argument unless it was one of the special keywords 'any' or 'none', causing the permission list to fail open if only one permission was specified.
... continues on next page ...

...continued from previous page ...

Vulnerability Detection Method

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

Details: OpenBSD OpenSSH 8.7 - 9.1 Unspecified Vulnerability

OID:1.3.6.1.4.1.25623.1.0.104511

Version used: 2025-01-21T05:37:33Z

Product Detection Result

Product: cpe:/a:openbsd:openssh:8.9p1

Method: OpenSSH Detection Consolidation

OID: 1.3.6.1.4.1.25623.1.0.108577)

Referencesurl: <https://www.openssh.com/releases/notes.html#9.2>url: <https://www.openwall.com/lists/oss-security/2023/02/02/3>

Medium (CVSS: 5.0)

NVT: OpenBSD OpenSSH 8.7 - 9.1 Unspecified Vulnerability

Product detection result

cpe:/a:openbsd:openssh:8.9p1

Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

Summary

OpenBSD OpenSSH is prone to an unspecified vulnerability.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 8.9p1

Fixed version: 9.2

Installation

path / port: /snap/core22/1612/usr/sbin/sshd

Solution:**Solution type:** VendorFix

Update to version 9.2 or later.

Affected Software/OS

OpenBSD OpenSSH versions starting from 8.7 and prior to 9.2.

Vulnerability Insight

... continues on next page ...

...continued from previous page ...
The PermitRemoteOpen option would ignore its first argument unless it was one of the special keywords 'any' or 'none', causing the permission list to fail open if only one permission was specified.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH 8.7 - 9.1 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104511 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releasenotes.html#9.2 url: https://www.openwall.com/lists/oss-security/2023/02/02/3

Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH 8.7 - 9.1 Unspecified Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.2 Installation path / port: /snap/core22/1748/usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.2 or later.
Affected Software/OS OpenBSD OpenSSH versions starting from 8.7 and prior to 9.2.
... continues on next page ...

...continued from previous page ...

Vulnerability Insight

The PermitRemoteOpen option would ignore its first argument unless it was one of the special keywords 'any' or 'none', causing the permission list to fail open if only one permission was specified.

Vulnerability Detection Method

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

Details: OpenBSD OpenSSH 8.7 - 9.1 Unspecified Vulnerability

OID:1.3.6.1.4.1.25623.1.0.104511

Version used: 2025-01-21T05:37:33Z

Product Detection Result

Product: cpe:/a:openbsd:openssh:8.9p1

Method: OpenSSH Detection Consolidation

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

url: <https://www.openssh.com/releasenotes.html#9.2>

url: <https://www.openwall.com/lists/oss-security/2023/02/02/3>

Medium (CVSS: 5.0)

NVT: OpenBSD OpenSSH 8.7 - 9.1 Unspecified Vulnerability

Product detection result

cpe:/a:openbsd:openssh:8.9p1

Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

Summary

OpenBSD OpenSSH is prone to an unspecified vulnerability.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 8.9p1

Fixed version: 9.2

Installation

path / port: /snap/core22/1748/usr/sbin/sshd

Solution:

Solution type: VendorFix

Update to version 9.2 or later.

... continues on next page ...

...continued from previous page ...
Affected Software/OS OpenBSD OpenSSH versions starting from 8.7 and prior to 9.2.
Vulnerability Insight The PermitRemoteOpen option would ignore its first argument unless it was one of the special keywords 'any' or 'none', causing the permission list to fail open if only one permission was specified.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH 8.7 - 9.1 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104511 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releasenotes.html#9.2 url: https://www.openwall.com/lists/oss-security/2023/02/02/3
Medium (CVSS: 4.6) NVT: Missing Linux Kernel mitigations for 'Register File Data Sampling (RFDS)' hardware vulnerability (INTEL-SA-00898)
Product detection result cpe:/a:linux:kernel Detected by Detection of Linux Kernel mitigation status for hardware vulnerabili ↔ties (OID: 1.3.6.1.4.1.25623.1.0.108765)
Summary The remote host is missing one or more known mitigation(s) on Linux Kernel side for the refer- enced 'Register File Data Sampling (RFDS)' hardware vulnerability.
Quality of Detection (QoD): 80%
Vulnerability Detection Result The Linux Kernel on the remote host is missing the mitigation for the "reg_file_ ↔data_sampling" hardware vulnerability as reported by the sysfs interface: sysfs file checked Linux Kernel st ↔atus (SSH response) ----- ↔----- ... continues on next page ...

...continued from previous page...	
<pre>/sys/devices/system/cpu/vulnerabilities/reg_file_data_sampling Vulnerable: No ↪microcode</pre> <p>Notes on the "Linux Kernel status (SSH response)" column:</p> <ul style="list-style-type: none">- sysfs file missing: The sysfs interface is available but the sysfs file for this specific vulnerability is missing. This means the current Linux Kernel does not know this vulnerability yet. Based on this it is assumed that it doesn't provide any mitigation and that the target system is vulnerable.- Strings including "Mitigation:", "Not affected" or "Vulnerable" are reported directly by the Linux Kernel.- All other strings are responses to various SSH commands.	
<p>Solution:</p> <p>Solution type: VendorFix</p> <p>The following solutions exist:</p> <ul style="list-style-type: none">- Update to a more recent Linux Kernel to receive mitigations on Kernel level and info about the mitigation status from it- Enable the mitigation(s) in the Linux Kernel (might be disabled depending on the configuration) <p>Additional possible mitigations (if provided by the vendor) are to:</p> <ul style="list-style-type: none">- install a Microcode update- update the BIOS of the Mainboard <p>Note: Please create an override for this result if one of the following applies:</p> <ul style="list-style-type: none">- the sysfs file is not available but other mitigations like a Microcode update is already in place- the sysfs file is not available but the CPU of the host is not affected- the reporting of the Linux Kernel is not correct (this is out of the control of this VT)	
<p>Affected Software/OS</p> <p>Various Intel CPUs. Please see the references for the full list of affected CPUs.</p>	
<p>Vulnerability Detection Method</p> <p>Checks previous gathered information on the mitigation status reported by the Linux Kernel.</p> <p>Details: Missing Linux Kernel mitigations for 'Register File Data Sampling (RFDS)' hardware.</p> <p>↪...</p> <p>OID:1.3.6.1.4.1.25623.1.0.114456</p> <p>Version used: 2024-06-14T05:05:48Z</p>	
<p>Product Detection Result</p> <p>Product: cpe:/a:linux:kernel</p> <p>Method: Detection of Linux Kernel mitigation status for hardware vulnerabilities</p> <p>OID: 1.3.6.1.4.1.25623.1.0.108765)</p>	
<p>References</p> <p>cve: CVE-2023-28746</p> <p>url: https://docs.kernel.org/admin-guide/hw-vuln/reg-file-data-sampling.html</p> <p>url: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-000898.html</p> <p>↪0898.html</p>	
...continues on next page...	

...continued from previous page ...
url: https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/processors-affected-consolidated-product-cpu-model.html↵
url: https://www.intel.com/content/www/us/en/developer/articles/technical/software-re-security-guidance/advisory-guidance/register-file-data-sampling.html↵
cert-bund: WID-SEC-2024-1913
cert-bund: WID-SEC-2024-0619
cert-bund: WID-SEC-2024-0615
dfn-cert: DFN-CERT-2024-3416
dfn-cert: DFN-CERT-2024-2999
dfn-cert: DFN-CERT-2024-2750
dfn-cert: DFN-CERT-2024-2748
dfn-cert: DFN-CERT-2024-2175
dfn-cert: DFN-CERT-2024-2173
dfn-cert: DFN-CERT-2024-2033
dfn-cert: DFN-CERT-2024-1850
dfn-cert: DFN-CERT-2024-1448
dfn-cert: DFN-CERT-2024-1444
dfn-cert: DFN-CERT-2024-1309
dfn-cert: DFN-CERT-2024-1304
dfn-cert: DFN-CERT-2024-1202
dfn-cert: DFN-CERT-2024-1173
dfn-cert: DFN-CERT-2024-1122
dfn-cert: DFN-CERT-2024-1039
dfn-cert: DFN-CERT-2024-1024
dfn-cert: DFN-CERT-2024-1023
dfn-cert: DFN-CERT-2024-0986
dfn-cert: DFN-CERT-2024-0910
dfn-cert: DFN-CERT-2024-0780
dfn-cert: DFN-CERT-2024-0773
dfn-cert: DFN-CERT-2024-0772
dfn-cert: DFN-CERT-2024-0771
dfn-cert: DFN-CERT-2024-0770
dfn-cert: DFN-CERT-2024-0708
dfn-cert: DFN-CERT-2024-0690
dfn-cert: DFN-CERT-2024-0689
dfn-cert: DFN-CERT-2024-0678
dfn-cert: DFN-CERT-2024-0666
dfn-cert: DFN-CERT-2024-0665
dfn-cert: DFN-CERT-2024-0628

Medium (CVSS: 4.3) NVT: PHP < 8.0.29, 8.1.x < 8.1.20, 8.2.x < 8.2.7 Security Update - Linux
Product detection result cpe:/a:php:php:7.2.34 Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
... continues on next page ...

...continued from previous page ...
Summary PHP is prone to a missing error check and insufficient random bytes in HTTP Digest authentication for SOAP vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 7.2.34 Fixed version: 8.0.29 Installation path / port: /usr/bin/php7.2
Solution: Solution type: VendorFix Update to version 8.0.29, 8.1.10, 8.2.7 or later.
Affected Software/OS PHP prior to version 8.0.29, 8.1.x prior to 8.1.20 and 8.2.x prior to 8.2.7.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP < 8.0.29, 8.1.x < 8.1.20, 8.2.x < 8.2.7 Security Update - Linux OID:1.3.6.1.4.1.25623.1.0.149760 Version used: 2023-10-13T05:06:10Z
Product Detection Result Product: cpe:/a:php:php:7.2.34 Method: PHP Detection (HTTP) OID: 1.3.6.1.4.1.25623.1.0.800109)
References cve: CVE-2023-3247 url: https://www.php.net/ChangeLog-8.php#8.0.29 url: https://www.php.net/ChangeLog-8.php#8.1.20 url: https://www.php.net/ChangeLog-8.php#8.2.7 url: https://github.com/php/php-src/security/advisories/GHSA-76gg-c692-v2mw cert-bund: WID-SEC-2023-2917 cert-bund: WID-SEC-2023-2680 cert-bund: WID-SEC-2023-1506 dfn-cert: DFN-CERT-2024-3330 dfn-cert: DFN-CERT-2023-2570 dfn-cert: DFN-CERT-2023-2542 dfn-cert: DFN-CERT-2023-1328

Medium (CVSS: 4.3) NVT: Samba Information Leak Vulnerability (CVE-2018-14628)
Product detection result cpe:/a:samba:samba:4.15.13 Detected by Samba Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800403)
Summary Samba is prone to an information leak vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 4.15.13 Fixed version: 4.18.9 Installation path / port: /usr/sbin/smbd
Solution: Solution type: VendorFix Update to version 4.18.9, 4.19.3 or later.
Affected Software/OS Samba versions from 4.0.0 onwards.
Vulnerability Insight Samba is vulnerable to an information leak (compared with the established behaviour of Microsoft's Active Directory) when Samba is an Active Directory Domain Controller. Missing access control checks on the LDAP_SERVER_SHOW_DELETED_OID control in the DSDB database layer cause the LDAP server to disclose, to authenticated but not privileged users, the names and preserved attributes of deleted objects. (Microsoft AD simply does not return these objects on a search). No information that was hidden before the deletion is visible, but in Microsoft Active Directory the whole object is also not visible without administrative rights, whereas Samba allows read of limited set of attributes that are preserved after delete. There is no further vulnerability associated with this error, merely an information disclosure.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Samba Information Leak Vulnerability (CVE-2018-14628) OID:1.3.6.1.4.1.25623.1.0.104503 Version used: 2023-11-30T05:06:26Z
Product Detection Result Product: cpe:/a:samba:samba:4.15.13 Method: Samba Version Detection
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.800403)
References cve: CVE-2018-14628 url: https://www.samba.org/samba/history/samba-4.19.3.html url: https://www.samba.org/samba/history/samba-4.18.9.html url: https://www.samba.org/samba/security/CVE-2018-14628.html url: https://bugzilla.samba.org/show_bug.cgi?id=13595 url: https://bugzilla.redhat.com/show_bug.cgi?id=1625445 cert-bund: WID-SEC-2023-3012 dfn-cert: DFN-CERT-2023-2993
Medium (CVSS: 4.0) NVT: OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.1 Installation path / port: /snap/core22/1748/usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.1 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.1.
Vulnerability Insight The following vulnerabilities exist: - A one-byte overflow in SSH- banner processing in ssh-keyscan. - A double free() in error path of file hashing step in signing/verify code in ssh-keygen. - A double-free in error path in ssh-keysign.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.127244 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releases.html#9.1

Medium (CVSS: 4.0) NVT: OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.1 Installation path / port: /usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.1 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.1.
Vulnerability Insight The following vulnerabilities exist: - A one-byte overflow in SSH- banner processing in ssh-keyscan. - A double free() in error path of file hashing step in signing/verify code in ssh-keygen.
... continues on next page ...

...continued from previous page ...
- A double-free in error path in ssh-keysign.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.127244 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releasenotes.html#9.1

Medium (CVSS: 4.0) NVT: OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.1 Installation path / port: /snap/core22/1748/usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.1 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.1.
Vulnerability Insight The following vulnerabilities exist: ... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - A one-byte overflow in SSH- banner processing in ssh-keyscan. - A double free() in error path of file hashing step in signing/verify code in ssh-keygen. - A double-free in error path in ssh-keysign.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.127244 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releasenotes.html#9.1

Medium (CVSS: 4.0) NVT: OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.1 Installation path / port: /usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.1 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.1.
... continues on next page ...

...continued from previous page ...
Vulnerability Insight The following vulnerabilities exist: <ul style="list-style-type: none"> - A one-byte overflow in SSH- banner processing in ssh-keyscan. - A double free() in error path of file hashing step in signing/verify code in ssh-keygen. - A double-free in error path in ssh-keysign.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.127244 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releasenotes.html#9.1

Medium (CVSS: 4.0) NVT: OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.1 Installation path / port: /snap/core22/1612/usr/bin/ssh
Solution: Solution type: VendorFix Update to version 9.1 or later.
Affected Software/OS ... continues on next page ...

...continued from previous page ...
OpenBSD OpenSSH prior to version 9.1.
Vulnerability Insight The following vulnerabilities exist: <ul style="list-style-type: none"> - A one-byte overflow in SSH- banner processing in ssh-keyscan. - A double free() in error path of file hashing step in signing/verify code in ssh-keygen. - A double-free in error path in ssh-keysign.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.127244 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releasenotes.html#9.1

Medium (CVSS: 4.0) NVT: OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.1 Installation path / port: /snap/core22/1612/usr/sbin/sshd
Solution: Solution type: VendorFix Update to version 9.1 or later.
... continues on next page ...

...continued from previous page ...
Affected Software/OS OpenBSD OpenSSH prior to version 9.1.
Vulnerability Insight The following vulnerabilities exist: - A one-byte overflow in SSH- banner processing in ssh-keyscan. - A double free() in error path of file hashing step in signing/verify code in ssh-keygen. - A double-free in error path in ssh-keysign.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.127244 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releasenotes.html#9.1

[\[return to 10.0.0.92 \]](#)

2.2.10 Medium 22/tcp

Medium (CVSS: 6.5) NVT: OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities (Terrapin Attack)
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to multiple vulnerabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.6 Installation
... continues on next page ...

...continued from previous page ...	
path / port:	22/tcp
Solution: Solution type: VendorFix Update to version 9.6 or later. Note: Client and Server implementations need to run a fixed version to mitigate the Terrapin flaw.	
Affected Software/OS OpenBSD OpenSSH prior to version 9.6.	
Vulnerability Insight The following vulnerabilities exist: - CVE-2023-48795: The SSH transport protocol with certain OpenSSH extensions allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a 'Terrapin attack'. - CVE-2023-51384: In ssh-agent certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys. - CVE-2023-51385: OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities (Terrapin Attack) OID:1.3.6.1.4.1.25623.1.0.118572 Version used: 2024-03-15T05:06:15Z	
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)	
References cve: CVE-2023-48795 cve: CVE-2023-51384 cve: CVE-2023-51385 url: https://www.openssh.com/txt/release-9.6 url: https://terrapin-attack.com url: https://vin01.github.io/piptagole/ssh/security/openssh/libssh/remote-code-e↵execution/2023/12/20/openssh-proxycommand-libssh-rce.html	
...continues on next page ...	

...continued from previous page ...

cert-bund: WID-SEC-2025-0168
 cert-bund: WID-SEC-2025-0144
 cert-bund: WID-SEC-2025-0139
 cert-bund: WID-SEC-2024-3377
 cert-bund: WID-SEC-2024-3320
 cert-bund: WID-SEC-2024-3198
 cert-bund: WID-SEC-2024-3195
 cert-bund: WID-SEC-2024-3140
 cert-bund: WID-SEC-2024-1913
 cert-bund: WID-SEC-2024-1781
 cert-bund: WID-SEC-2024-1701
 cert-bund: WID-SEC-2024-1656
 cert-bund: WID-SEC-2024-1655
 cert-bund: WID-SEC-2024-1643
 cert-bund: WID-SEC-2024-1642
 cert-bund: WID-SEC-2024-1639
 cert-bund: WID-SEC-2024-1637
 cert-bund: WID-SEC-2024-1630
 cert-bund: WID-SEC-2024-1474
 cert-bund: WID-SEC-2024-1248
 cert-bund: WID-SEC-2024-1228
 cert-bund: WID-SEC-2024-1186
 cert-bund: WID-SEC-2024-1082
 cert-bund: WID-SEC-2024-0899
 cert-bund: WID-SEC-2024-0892
 cert-bund: WID-SEC-2024-0889
 cert-bund: WID-SEC-2024-0885
 cert-bund: WID-SEC-2024-0874
 cert-bund: WID-SEC-2024-0869
 cert-bund: WID-SEC-2024-0578
 cert-bund: WID-SEC-2024-0564
 cert-bund: WID-SEC-2024-0523
 cert-bund: WID-SEC-2023-3182
 cert-bund: WID-SEC-2023-3174
 dfn-cert: DFN-CERT-2025-0294
 dfn-cert: DFN-CERT-2025-0173
 dfn-cert: DFN-CERT-2025-0165
 dfn-cert: DFN-CERT-2025-0024
 dfn-cert: DFN-CERT-2024-3171
 dfn-cert: DFN-CERT-2024-2818
 dfn-cert: DFN-CERT-2024-2759
 dfn-cert: DFN-CERT-2024-2741
 dfn-cert: DFN-CERT-2024-2682
 dfn-cert: DFN-CERT-2024-2602
 dfn-cert: DFN-CERT-2024-2573
 dfn-cert: DFN-CERT-2024-2392
 dfn-cert: DFN-CERT-2024-2210

...continues on next page ...

...continued from previous page ...	
dfn-cert:	DFN-CERT-2024-2209
dfn-cert:	DFN-CERT-2024-2194
dfn-cert:	DFN-CERT-2024-2169
dfn-cert:	DFN-CERT-2024-2048
dfn-cert:	DFN-CERT-2024-2030
dfn-cert:	DFN-CERT-2024-2028
dfn-cert:	DFN-CERT-2024-1930
dfn-cert:	DFN-CERT-2024-1895
dfn-cert:	DFN-CERT-2024-1869
dfn-cert:	DFN-CERT-2024-1868
dfn-cert:	DFN-CERT-2024-1865
dfn-cert:	DFN-CERT-2024-1862
dfn-cert:	DFN-CERT-2024-1854
dfn-cert:	DFN-CERT-2024-1846
dfn-cert:	DFN-CERT-2024-1817
dfn-cert:	DFN-CERT-2024-1794
dfn-cert:	DFN-CERT-2024-1715
dfn-cert:	DFN-CERT-2024-1698
dfn-cert:	DFN-CERT-2024-1688
dfn-cert:	DFN-CERT-2024-1655
dfn-cert:	DFN-CERT-2024-1600
dfn-cert:	DFN-CERT-2024-1443
dfn-cert:	DFN-CERT-2024-1442
dfn-cert:	DFN-CERT-2024-1413
dfn-cert:	DFN-CERT-2024-1382
dfn-cert:	DFN-CERT-2024-1380
dfn-cert:	DFN-CERT-2024-1373
dfn-cert:	DFN-CERT-2024-1260
dfn-cert:	DFN-CERT-2024-1259
dfn-cert:	DFN-CERT-2024-1108
dfn-cert:	DFN-CERT-2024-1061
dfn-cert:	DFN-CERT-2024-1029
dfn-cert:	DFN-CERT-2024-1003
dfn-cert:	DFN-CERT-2024-1000
dfn-cert:	DFN-CERT-2024-0896
dfn-cert:	DFN-CERT-2024-0779
dfn-cert:	DFN-CERT-2024-0762
dfn-cert:	DFN-CERT-2024-0744
dfn-cert:	DFN-CERT-2024-0698
dfn-cert:	DFN-CERT-2024-0633
dfn-cert:	DFN-CERT-2024-0619
dfn-cert:	DFN-CERT-2024-0618
dfn-cert:	DFN-CERT-2024-0616
dfn-cert:	DFN-CERT-2024-0597
dfn-cert:	DFN-CERT-2024-0545
dfn-cert:	DFN-CERT-2024-0526
dfn-cert:	DFN-CERT-2024-0491
...continues on next page ...	

...continued from previous page ...
dfn-cert: DFN-CERT-2024-0480
dfn-cert: DFN-CERT-2024-0451
dfn-cert: DFN-CERT-2024-0440
dfn-cert: DFN-CERT-2024-0420
dfn-cert: DFN-CERT-2024-0388
dfn-cert: DFN-CERT-2024-0343
dfn-cert: DFN-CERT-2024-0306
dfn-cert: DFN-CERT-2024-0299
dfn-cert: DFN-CERT-2024-0285
dfn-cert: DFN-CERT-2024-0267
dfn-cert: DFN-CERT-2024-0251
dfn-cert: DFN-CERT-2024-0215
dfn-cert: DFN-CERT-2024-0211
dfn-cert: DFN-CERT-2024-0164
dfn-cert: DFN-CERT-2024-0154
dfn-cert: DFN-CERT-2024-0101
dfn-cert: DFN-CERT-2024-0092
dfn-cert: DFN-CERT-2024-0088
dfn-cert: DFN-CERT-2024-0067
dfn-cert: DFN-CERT-2024-0063
dfn-cert: DFN-CERT-2024-0062
dfn-cert: DFN-CERT-2024-0024
dfn-cert: DFN-CERT-2024-0022
dfn-cert: DFN-CERT-2024-0013
dfn-cert: DFN-CERT-2023-3219
dfn-cert: DFN-CERT-2023-3218
dfn-cert: DFN-CERT-2023-3210
dfn-cert: DFN-CERT-2023-3201
dfn-cert: DFN-CERT-2023-3200
dfn-cert: DFN-CERT-2023-3195
dfn-cert: DFN-CERT-2023-3193
dfn-cert: DFN-CERT-2023-3191
dfn-cert: DFN-CERT-2023-3185
dfn-cert: DFN-CERT-2023-3184
dfn-cert: DFN-CERT-2023-3183
dfn-cert: DFN-CERT-2023-3182
dfn-cert: DFN-CERT-2023-3175

Medium (CVSS: 5.9) NVT: Prefix Truncation Attacks in SSH Specification (Terrapin Attack)
Product detection result cpe:/a:ietf:secure_shell_protocol Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↔)
... continues on next page ...

...continued from previous page ...
Summary The remote SSH server is supporting an specific encryption algorithm or MAC. Parts of their SSH specification are vulnerable to a novel prefix truncation attack (a.k.a. Terrapin attack).
Quality of Detection (QoD): 30%
Vulnerability Detection Result The remote SSH server supports the following possible affected client-to-server ↪ encryption algorithm(s): chacha20-poly1305@openssh.com The remote SSH server supports the following possible affected server-to-client ↪ encryption algorithm(s): chacha20-poly1305@openssh.com The remote SSH server supports the following "strict kex" algorithm as a possible ↪ mitigation: kex-strict-s-v00@openssh.com
Solution: Solution type: VendorFix - Update OpenSSH to version 9.6 or later - For other products please contact the vendor for possible fixes / updates Mitigation: - To mitigate this protocol vulnerability, OpenSSH suggested a so-called 'strict kex' which alters the SSH handshake to ensure a Man-in-the-Middle attacker cannot introduce unauthenticated messages as well as convey sequence number manipulation across handshakes. Support for strict key exchange has been added to a variety of SSH implementations, including OpenSSH itself, PuTTY, libssh, and more. Warning: To take effect, both the client and server must support this countermeasure. As a stop-gap measure, peers may also (temporarily) disable the affected algorithms and use unaffected alternatives like AES-GCM instead until patches are available.
Affected Software/OS Systems supporting the following encryption algorithm and/or MACs: - ChaCha20-Poly1305 (chacha20-poly1305@openssh.com) encryption algorithm - CBC encryption algorithm and Encrypt-then-MAC (*-etm@openssh.com) MAC
Vulnerability Insight Parts of the SSH specification are vulnerable to a novel prefix truncation attack (a.k.a. Terrapin attack), which allows a man-in-the-middle attacker to strip an arbitrary number of messages right after the initial key exchange, breaking SSH extension negotiation (RFC8308) in the process and thus downgrading connection security.
Vulnerability Detection Method Checks the supported algorithms and MACs of the remote SSH server. Note: This VT has a low QoD because mitigation is possible / available via software updates.
... continues on next page ...

...continued from previous page...
Details: Prefix Truncation Attacks in SSH Specification (Terrapin Attack) OID:1.3.6.1.4.1.25623.1.0.114238 Version used: 2024-06-14T05:05:48Z
Product Detection Result Product: cpe:/a:ietf:secure_shell_protocol Method: SSH Protocol Algorithms Supported OID: 1.3.6.1.4.1.25623.1.0.105565)
References cve: CVE-2023-48795 url: https://terrapin-attack.com url: https://www.openssh.com/txt/release-9.6 cert-bund: WID-SEC-2025-0168 cert-bund: WID-SEC-2025-0144 cert-bund: WID-SEC-2025-0139 cert-bund: WID-SEC-2024-3377 cert-bund: WID-SEC-2024-3320 cert-bund: WID-SEC-2024-3198 cert-bund: WID-SEC-2024-3195 cert-bund: WID-SEC-2024-1913 cert-bund: WID-SEC-2024-1781 cert-bund: WID-SEC-2024-1701 cert-bund: WID-SEC-2024-1656 cert-bund: WID-SEC-2024-1655 cert-bund: WID-SEC-2024-1643 cert-bund: WID-SEC-2024-1642 cert-bund: WID-SEC-2024-1639 cert-bund: WID-SEC-2024-1637 cert-bund: WID-SEC-2024-1630 cert-bund: WID-SEC-2024-1474 cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2024-1228 cert-bund: WID-SEC-2024-1186 cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2024-0899 cert-bund: WID-SEC-2024-0892 cert-bund: WID-SEC-2024-0889 cert-bund: WID-SEC-2024-0885 cert-bund: WID-SEC-2024-0874 cert-bund: WID-SEC-2024-0869 cert-bund: WID-SEC-2024-0578 cert-bund: WID-SEC-2024-0564 cert-bund: WID-SEC-2024-0523 cert-bund: WID-SEC-2023-3174 dfn-cert: DFN-CERT-2025-0294
...continues on next page...

...continued from previous page ...	
dfn-cert:	DFN-CERT-2025-0173
dfn-cert:	DFN-CERT-2025-0165
dfn-cert:	DFN-CERT-2025-0024
dfn-cert:	DFN-CERT-2024-3171
dfn-cert:	DFN-CERT-2024-2818
dfn-cert:	DFN-CERT-2024-2759
dfn-cert:	DFN-CERT-2024-2741
dfn-cert:	DFN-CERT-2024-2602
dfn-cert:	DFN-CERT-2024-2573
dfn-cert:	DFN-CERT-2024-2392
dfn-cert:	DFN-CERT-2024-2210
dfn-cert:	DFN-CERT-2024-2209
dfn-cert:	DFN-CERT-2024-2194
dfn-cert:	DFN-CERT-2024-2169
dfn-cert:	DFN-CERT-2024-2048
dfn-cert:	DFN-CERT-2024-2030
dfn-cert:	DFN-CERT-2024-2028
dfn-cert:	DFN-CERT-2024-1930
dfn-cert:	DFN-CERT-2024-1895
dfn-cert:	DFN-CERT-2024-1869
dfn-cert:	DFN-CERT-2024-1868
dfn-cert:	DFN-CERT-2024-1865
dfn-cert:	DFN-CERT-2024-1862
dfn-cert:	DFN-CERT-2024-1854
dfn-cert:	DFN-CERT-2024-1846
dfn-cert:	DFN-CERT-2024-1817
dfn-cert:	DFN-CERT-2024-1715
dfn-cert:	DFN-CERT-2024-1698
dfn-cert:	DFN-CERT-2024-1688
dfn-cert:	DFN-CERT-2024-1655
dfn-cert:	DFN-CERT-2024-1600
dfn-cert:	DFN-CERT-2024-1443
dfn-cert:	DFN-CERT-2024-1442
dfn-cert:	DFN-CERT-2024-1413
dfn-cert:	DFN-CERT-2024-1382
dfn-cert:	DFN-CERT-2024-1380
dfn-cert:	DFN-CERT-2024-1373
dfn-cert:	DFN-CERT-2024-1260
dfn-cert:	DFN-CERT-2024-1259
dfn-cert:	DFN-CERT-2024-1108
dfn-cert:	DFN-CERT-2024-1061
dfn-cert:	DFN-CERT-2024-1029
dfn-cert:	DFN-CERT-2024-1003
dfn-cert:	DFN-CERT-2024-1000
dfn-cert:	DFN-CERT-2024-0896
dfn-cert:	DFN-CERT-2024-0779
dfn-cert:	DFN-CERT-2024-0762
...continues on next page ...	

...continued from previous page ...

dfn-cert: DFN-CERT-2024-0744
dfn-cert: DFN-CERT-2024-0698
dfn-cert: DFN-CERT-2024-0633
dfn-cert: DFN-CERT-2024-0619
dfn-cert: DFN-CERT-2024-0618
dfn-cert: DFN-CERT-2024-0616
dfn-cert: DFN-CERT-2024-0597
dfn-cert: DFN-CERT-2024-0545
dfn-cert: DFN-CERT-2024-0526
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0451
dfn-cert: DFN-CERT-2024-0440
dfn-cert: DFN-CERT-2024-0420
dfn-cert: DFN-CERT-2024-0388
dfn-cert: DFN-CERT-2024-0343
dfn-cert: DFN-CERT-2024-0306
dfn-cert: DFN-CERT-2024-0299
dfn-cert: DFN-CERT-2024-0285
dfn-cert: DFN-CERT-2024-0267
dfn-cert: DFN-CERT-2024-0251
dfn-cert: DFN-CERT-2024-0215
dfn-cert: DFN-CERT-2024-0211
dfn-cert: DFN-CERT-2024-0164
dfn-cert: DFN-CERT-2024-0154
dfn-cert: DFN-CERT-2024-0101
dfn-cert: DFN-CERT-2024-0092
dfn-cert: DFN-CERT-2024-0088
dfn-cert: DFN-CERT-2024-0067
dfn-cert: DFN-CERT-2024-0063
dfn-cert: DFN-CERT-2024-0062
dfn-cert: DFN-CERT-2024-0024
dfn-cert: DFN-CERT-2024-0013
dfn-cert: DFN-CERT-2023-3219
dfn-cert: DFN-CERT-2023-3218
dfn-cert: DFN-CERT-2023-3210
dfn-cert: DFN-CERT-2023-3201
dfn-cert: DFN-CERT-2023-3200
dfn-cert: DFN-CERT-2023-3195
dfn-cert: DFN-CERT-2023-3193
dfn-cert: DFN-CERT-2023-3191
dfn-cert: DFN-CERT-2023-3185
dfn-cert: DFN-CERT-2023-3184
dfn-cert: DFN-CERT-2023-3183
dfn-cert: DFN-CERT-2023-3182
dfn-cert: DFN-CERT-2023-3175

Medium (CVSS: 5.3) NVT: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an information disclosure vulnerability.
Quality of Detection (QoD): 50%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: None Installation path / port: 22/tcp
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 All currently OpenSSH versions are known to be affected.
Vulnerability Insight OpenSSH allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012) OID:1.3.6.1.4.1.25623.1.0.117777 Version used: 2022-11-24T10:18:54Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References cve: CVE-2016-20012
... continues on next page ...

...continued from previous page ...
url: https://github.com/openssh/openssh-portable/pull/270 url: https://rushter.com/blog/public-ssh-keys/ url: https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak cert-bund: WID-SEC-2024-1082 cert-bund: WID-SEC-2024-0229 cert-bund: CB-K21/0979 dfn-cert: DFN-CERT-2024-1260

Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH 8.7 - 9.1 Unspecified Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.2 Installation path / port: 22/tcp
Solution: Solution type: VendorFix Update to version 9.2 or later.
Affected Software/OS OpenBSD OpenSSH versions starting from 8.7 and prior to 9.2.
Vulnerability Insight The PermitRemoteOpen option would ignore its first argument unless it was one of the special keywords 'any' or 'none', causing the permission list to fail open if only one permission was specified.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH 8.7 - 9.1 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104511 Version used: 2025-01-21T05:37:33Z
... continues on next page ...

...continued from previous page ...
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releases/notes.html#9.2 url: https://www.openwall.com/lists/oss-security/2023/02/02/3

Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH < 9.2 Unspecified Vulnerability
Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.2 Installation path / port: 22/tcp
Solution: Solution type: VendorFix Update to version 9.2 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.2.
Vulnerability Insight If the CanonicalizeHostname and CanonicalizePermittedCNAMEs options were enabled, and the system/libc resolver did not check that names in DNS responses were valid, then use of these options could allow an attacker with control of DNS to include invalid characters (possibly including wildcards) in names added to known_hosts files when they were updated. These names would still have to match the CanonicalizePermittedCNAMEs allow-list, so practical exploitation appears unlikely.
Vulnerability Detection Method ... continues on next page ...

...continued from previous page ...
<p>Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.2 Unspecified Vulnerability OID:1.3.6.1.4.1.25623.1.0.104512 Version used: 2025-01-21T05:37:33Z</p>
<p>Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>References url: https://www.openssh.com/releases/notes.html#9.2 url: https://www.openwall.com/lists/oss-security/2023/02/02/3</p>

<p>Medium (CVSS: 5.0) NVT: OpenBSD OpenSSH < 9.3 Unspecified Vulnerability</p>
<p>Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>Summary OpenBSD OpenSSH is prone to an unspecified vulnerability.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.3 Installation path / port: 22/tcp</p>
<p>Solution: Solution type: VendorFix Update to version 9.3 or later.</p>
<p>Affected Software/OS OpenBSD OpenSSH prior to version 9.3.</p>
<p>Vulnerability Insight ... continues on next page ...</p>

...continued from previous page ...
<p>ssh(1): Portable OpenSSH provides an implementation of the getrrsetbyname(3) function if the standard library does not provide it, for use by the VerifyHostKeyDNS feature. A specifically crafted DNS response could cause this function to perform an out-of-bounds read of adjacent stack data, but this condition does not appear to be exploitable beyond denial-of-service to the ssh(1) client.</p> <p>The getrrsetbyname(3) replacement is only included if the system's standard library lacks this function and portable OpenSSH was not compiled with the ldns library (-with-ldns). getrrsetbyname(3) is only invoked if using VerifyHostKeyDNS to fetch SSHFP records. This problem was found by the Coverity static analyzer.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.3 Unspecified Vulnerability OID: 1.3.6.1.4.1.25623.1.0.104635 Version used: 2025-01-21T05:37:33Z</p>
<p>Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>References url: https://www.openssh.com/releasenotes.html#9.3 url: https://www.openwall.com/lists/oss-security/2023/03/15/8</p>

<p>Medium (CVSS: 4.0) NVT: OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities</p>
<p>Product detection result cpe:/a:openbsd:openssh:8.9p1 Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)</p>
<p>Summary OpenBSD OpenSSH is prone to multiple vulnerabilities.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result Installed version: 8.9p1 Fixed version: 9.1 Installation path / port: 22/tcp</p>
<p>Solution: Solution type: VendorFix</p>
... continues on next page ...

...continued from previous page ...
Update to version 9.1 or later.
Affected Software/OS OpenBSD OpenSSH prior to version 9.1.
Vulnerability Insight The following vulnerabilities exist: - A one-byte overflow in SSH- banner processing in ssh-keyscan. - A double free() in error path of file hashing step in signing/verify code in ssh-keygen. - A double-free in error path in ssh-keysign.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.127244 Version used: 2025-01-21T05:37:33Z
Product Detection Result Product: cpe:/a:openbsd:openssh:8.9p1 Method: OpenSSH Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.108577)
References url: https://www.openssh.com/releasenotes.html#9.1

[\[return to 10.0.0.92 \]](#)

2.2.11 Medium 25/tcp

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

[\[return to 10.0.0.92 \]](#)

2.2.12 Low general/tcp

Low (CVSS: 2.6) NVT: TCP Timestamps Information Disclosure
Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.
Quality of Detection (QoD): 80%
Vulnerability Detection Result It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 592921017 Packet 2: 592922094
Impact A side effect of this feature is that the uptime of the remote host can sometimes be computed.
Solution: Solution type: Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
... continues on next page ...

...continued from previous page ...
See the references for more information.
Affected Software/OS TCP implementations that implement RFC1323/RFC7323.
Vulnerability Insight The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
Vulnerability Detection Method Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
References url: https://datatracker.ietf.org/doc/html/rfc1323 url: https://datatracker.ietf.org/doc/html/rfc7323 url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152 url: https://www.fortiguard.com/psirt/FG-IR-16-090

[\[return to 10.0.0.92 \]](#)

2.2.13 Low 22/tcp

Low (CVSS: 2.6) NVT: Weak MAC Algorithm(s) Supported (SSH)
Product detection result cpe:/a:ietf:secure_shell_protocol Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↪)
Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).
Quality of Detection (QoD): 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
... continues on next page ...

...continued from previous page ...
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: 2024-06-14T05:05:48Z
Product Detection Result Product: cpe:/a:ietf:secure_shell_protocol Method: SSH Protocol Algorithms Supported OID: 1.3.6.1.4.1.25623.1.0.105565)
References url: https://www.rfc-editor.org/rfc/rfc6668 url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[\[return to 10.0.0.92 \]](#)

2.2.14 Low general/icmp

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

...continued from previous page...	
<ul style="list-style-type: none"> - ICMP Type: 14 - ICMP Code: 0 	
Impact This information could theoretically be used to exploit weak time-based random number generators in other services.	
Solution: Solution type: Mitigation Various mitigations are possible: <ul style="list-style-type: none"> - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks) 	
Vulnerability Insight The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.	
Vulnerability Detection Method Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. Details: ICMP Timestamp Reply Information Disclosure OID:1.3.6.1.4.1.25623.1.0.103190 Version used: 2025-01-21T05:37:33Z	
References cve: CVE-1999-0524 url: https://datatracker.ietf.org/doc/html/rfc792 url: https://datatracker.ietf.org/doc/html/rfc2780 cert-bund: CB-K15/1514 cert-bund: CB-K14/0632 dfn-cert: DFN-CERT-2014-0658	

[\[return to 10.0.0.92 \]](#)

2.3 10.0.0.116

Host scan start Tue Mar 4 16:54:18 2025 UTC
Host scan end Tue Mar 4 17:59:53 2025 UTC

Service (Port)	Threat Level
443/tcp	High

2.3.1 High 443/tcp

High (CVSS: 10.0) NVT: Greenbone Security Assistant (GSA) Default Credentials (HTTP)
Summary The remote Greenbone Security Assistant (GSA) is installed / configured in a way that it has account(s) with default passwords enabled.
Quality of Detection (QoD): 100%
Vulnerability Detection Result It was possible to login using the following credentials (username:password): admin:admin
Impact This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.
Solution: Solution type: Workaround Change the password of the mentioned account(s).
Vulnerability Detection Method Tries to login with known default credentials via the HTTP protocol. Details: Greenbone Security Assistant (GSA) Default Credentials (HTTP) OID:1.3.6.1.4.1.25623.1.0.105354 Version used: 2024-07-10T05:05:27Z

[\[return to 10.0.0.116 \]](#)

2.4 10.0.0.1

Host scan start Tue Mar 4 16:54:18 2025 UTC
Host scan end Tue Mar 4 21:21:44 2025 UTC

Service (Port)	Threat Level
443/tcp	High
53/tcp	High
12865/tcp	Medium
443/tcp	Medium
53/tcp	Medium
80/tcp	Medium
general/icmp	Low
general/tcp	Low

2.4.1 High 443/tcp

<p>High (CVSS: 7.5) NVT: Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)</p>
<p>Product detection result cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.↪802067)</p>
<p>Summary The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result 'DHE' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256</p>
<p>Impact This vulnerability allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, also known as a D(HE)ater attack. There could be an increase in CPU usage in the affected component. For OpenSSH, users may observe issues such as a slowdown in SSH connections.</p>
<p>Solution: Solution type: Mitigation - DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.</p>
<p>Vulnerability Insight ... continues on next page ...</p>

<p>...continued from previous page ...</p> <ul style="list-style-type: none"> - CVE-2002-20001: The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE. - CVE-2022-40735: The Diffie-Hellman Key Agreement Protocol allows use of long exponents that arguably make certain calculations unnecessarily expensive, because the 1996 van Oorschot and Wiener paper found that '(appropriately) short exponents' can be used when there are adequate subgroup constraints, and these short exponents can lead to less expensive calculations than for long exponents. This issue is different from CVE-2002-20001 because it is based on an observation about exponent size, rather than an observation about numbers that are not public keys. The specific situations in which calculation expense would constitute a server-side vulnerability depend on the protocol (e.g., TLS, SSH, or IKE) and the DHE implementation details. In general, there might be an availability concern because of server-side resource consumption from DHE modular-exponentiation calculations. Finally, it is possible for an attacker to exploit this vulnerability and CVE-2002-20001 together. - CVE-2024-41996: Validating the order of the public keys in the Diffie-Hellman Key Agreement Protocol, when an approved safe prime is used, allows remote attackers (from the client side) to trigger unnecessarily expensive server-side DHE modular-exponentiation calculations. The client may cause asymmetric resource consumption. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE and validate the order of the public key.
<p>Vulnerability Detection Method Checks the supported cipher suites of the remote SSL/TLS server. Details: Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) OID:1.3.6.1.4.1.25623.1.0.117840 Version used: 2024-10-03T05:05:33Z</p>
<p>Product Detection Result Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Report Supported Cipher Suites OID: 1.3.6.1.4.1.25623.1.0.802067)</p>
<p>References cve: CVE-2002-20001 cve: CVE-2022-40735 cve: CVE-2024-41996 url: https://dheatattack.gitlab.io/ url: https://dheatattack.gitlab.io/details/ url: https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol url: https://github.com/Balasys/dheater url: https://github.com/c0r0n3r/dheater</p>
<p>...continues on next page ...</p>

...continued from previous page ...

```

cert-bund: WID-SEC-2024-3056
cert-bund: WID-SEC-2023-1886
cert-bund: WID-SEC-2023-1352
cert-bund: WID-SEC-2022-2251
cert-bund: WID-SEC-2022-2000
cert-bund: CB-K22/0224
cert-bund: CB-K21/1276
dfn-cert: DFN-CERT-2024-2847
dfn-cert: DFN-CERT-2024-2578
dfn-cert: DFN-CERT-2024-1671
dfn-cert: DFN-CERT-2023-1697
dfn-cert: DFN-CERT-2023-1332
dfn-cert: DFN-CERT-2022-2147
dfn-cert: DFN-CERT-2022-0437
dfn-cert: DFN-CERT-2021-2622

```

[\[return to 10.0.0.1 \]](#)

2.4.2 High 53/tcp

High (CVSS: 9.8)**NVT: Dnsmasq <= 2.86 Multiple Vulnerabilities****Product detection result**

cpe:/a:thekelleys:dnsmasq:2.83

Detected by Dnsmasq Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.117275)

Summary

Dnsmasq is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 2.83

Fixed version: 2.87

Installation

path / port: 53/tcp

Solution:**Solution type:** VendorFix

Update to version 2.87 or later.

Affected Software/OS

Dnsmasq version 2.86 and prior.

... continues on next page ...

...continued from previous page ...

Vulnerability Insight

The following flaws exist:

- CVE-2021-45951: Heap-based buffer overflow in check_bad_address
- CVE-2021-45952: Heap-based buffer overflow in dhcp_reply
- CVE-2021-45953: Heap-based buffer overflow in extract_name
- CVE-2021-45954: Heap-based buffer overflow in extract_name
- CVE-2021-45955: Heap-based buffer overflow in resize_packet
- CVE-2021-45956: Heap-based buffer overflow in print_mac
- CVE-2021-45957: Heap-based buffer overflow in answer_request

Note: The CVEs above have been changed to status 'DISPUTED'

- CVE-2022-0934: Heap use after free in dhcp6_no_relay

Vulnerability Detection Method

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

Details: Dnsmasq <= 2.86 Multiple Vulnerabilities

OID:1.3.6.1.4.1.25623.1.0.147385

Version used: 2023-01-12T10:12:15Z

Product Detection Result

Product: cpe:/a:thekelleys:dnsmasq:2.83

Method: Dnsmasq Detection Consolidation

OID: 1.3.6.1.4.1.25623.1.0.117275)

References

cve: CVE-2021-45951

cve: CVE-2021-45952

cve: CVE-2021-45953

cve: CVE-2021-45954

cve: CVE-2021-45955

cve: CVE-2021-45956

cve: CVE-2021-45957

cve: CVE-2022-0934

url: <https://github.com/google/oss-fuzz-vulns/blob/main/vulns/dnsmasq/OSV-2021-9↪24.yaml>

url: <https://github.com/google/oss-fuzz-vulns/blob/main/vulns/dnsmasq/OSV-2021-9↪27.yaml>

url: <https://github.com/google/oss-fuzz-vulns/blob/main/vulns/dnsmasq/OSV-2021-9↪29.yaml>

url: <https://github.com/google/oss-fuzz-vulns/blob/main/vulns/dnsmasq/OSV-2021-9↪31.yaml>

url: <https://github.com/google/oss-fuzz-vulns/blob/main/vulns/dnsmasq/OSV-2021-9↪32.yaml>

url: <https://github.com/google/oss-fuzz-vulns/blob/main/vulns/dnsmasq/OSV-2021-9↪33.yaml>

url: <https://github.com/google/oss-fuzz-vulns/blob/main/vulns/dnsmasq/OSV-2021-9>

...continues on next page ...

...continued from previous page ...
↔35.yaml url: https://lists.thekelleys.org.uk/pipermail/dnsmasq-discuss/2022q1/016272.htm ↔1 url: https://access.redhat.com/security/cve/cve-2022-0934 url: https://thekelleys.org.uk/dnsmasq/CHANGELOG cert-bund: WID-SEC-2024-0064 cert-bund: WID-SEC-2023-0137 cert-bund: WID-SEC-2022-1988 dfn-cert: DFN-CERT-2024-0829 dfn-cert: DFN-CERT-2022-0916 dfn-cert: DFN-CERT-2022-0906

High (CVSS: 7.5) NVT: Dnsmasq <= 2.89 UDP Fragmentation DoS Vulnerability
Product detection result cpe:/a:thekelleys:dnsmasq:2.83 Detected by Dnsmasq Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.117275)
Summary Dnsmasq is prone to a denial of service (DoS) vulnerability via an UDP Fragmentation attack.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 2.83 Fixed version: 2.90 Installation path / port: 53/tcp
Solution: Solution type: VendorFix Update to version 2.90 or later.
Affected Software/OS Dnsmasq version 2.89 and prior.
Vulnerability Insight The default maximum EDNS.0 UDP packet size was set to 4096 but should be 1232 because of DNS Flag Day 2020.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Dnsmasq <= 2.89 UDP Fragmentation DoS Vulnerability
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.104641 Version used: 2024-03-13T05:05:57Z
Product Detection Result Product: cpe:/a:thekelleys:dnsmaq:2.83 Method: Dnsmaq Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117275)
References cve: CVE-2023-28450 url: https://thekelleys.org.uk/gitweb/?p=dnsmaq.git;a=commit;h=eb92fb32b746f210↵4b0f370b5b295bb8dd4bd5e5 url: https://thekelleys.org.uk/dnsmaq/CHANGELOG url: https://www.dnsflagday.net/2020/ cert-bund: WID-SEC-2023-2917 cert-bund: WID-SEC-2023-0668 dfn-cert: DFN-CERT-2024-0829 dfn-cert: DFN-CERT-2024-0498 dfn-cert: DFN-CERT-2023-1947 dfn-cert: DFN-CERT-2023-0927

High (CVSS: 7.5) NVT: Dnsmaq < 2.90 Multiple DoS Vulnerabilities (KeyTrap)
Product detection result cpe:/a:thekelleys:dnsmaq:2.83 Detected by Dnsmaq Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.117275)
Summary Dnsmaq is prone to multiple denial of service (DoS) vulenrabilities.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 2.83 Fixed version: 2.90 Installation path / port: 53/tcp
Solution: Solution type: VendorFix Update to version 2.90 or later.
Affected Software/OS
... continues on next page ...

...continued from previous page ...
Dnsmasq version 2.89 and prior.
Vulnerability Insight Certain DNSSEC aspects of the DNS protocol (in RFC 4035 and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses when there is a zone with many DNSKEY and RRSIG records, aka the 'KeyTrap' issue. The protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Dnsmasq < 2.90 Multiple DoS Vulnerabilities (KeyTrap) OID:1.3.6.1.4.1.25623.1.0.151740 Version used: 2024-02-21T05:06:27Z
Product Detection Result Product: cpe:/a:thekelleys:dnsmasq:2.83 Method: Dnsmasq Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117275)
References cve: CVE-2023-50387 cve: CVE-2023-50868 url: https://thekelleys.org.uk/dnsmasq/CHANGELOG url: https://www.athene-center.de/en/keytrap cert-bund: WID-SEC-2025-0148 cert-bund: WID-SEC-2024-1347 cert-bund: WID-SEC-2024-1313 cert-bund: WID-SEC-2024-1307 cert-bund: WID-SEC-2024-1248 cert-bund: WID-SEC-2024-1226 cert-bund: WID-SEC-2024-1086 cert-bund: WID-SEC-2024-0387 cert-bund: WID-SEC-2024-0386 dfn-cert: DFN-CERT-2025-0041 dfn-cert: DFN-CERT-2025-0010 dfn-cert: DFN-CERT-2024-2264 dfn-cert: DFN-CERT-2024-1904 dfn-cert: DFN-CERT-2024-1523 dfn-cert: DFN-CERT-2024-1516 dfn-cert: DFN-CERT-2024-1474 dfn-cert: DFN-CERT-2024-1413 dfn-cert: DFN-CERT-2024-1223 dfn-cert: DFN-CERT-2024-1011 dfn-cert: DFN-CERT-2024-0984 dfn-cert: DFN-CERT-2024-0977
... continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2024-0921
dfn-cert: DFN-CERT-2024-0829
dfn-cert: DFN-CERT-2024-0529
dfn-cert: DFN-CERT-2024-0498
dfn-cert: DFN-CERT-2024-0404
dfn-cert: DFN-CERT-2024-0399
dfn-cert: DFN-CERT-2024-0387
dfn-cert: DFN-CERT-2024-0379
dfn-cert: DFN-CERT-2024-0375

[\[return to 10.0.0.1 \]](#)

2.4.3 Medium 12865/tcp

Medium (CVSS: 5.0) NVT: Check for Writesrv Service
Summary writesrv is running on this port, it is used to send messages to users.
Quality of Detection (QoD): 70%
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact This service gives potential attackers information about who is connected and who isn't, easing social engineering attacks for example.
Solution: Solution type: Mitigation Disable this service if you don't use it.
Vulnerability Detection Method Details: Check for Writesrv Service OID:1.3.6.1.4.1.25623.1.0.11222 Version used: 2023-08-01T13:29:10Z

[\[return to 10.0.0.1 \]](#)

2.4.4 Medium 443/tcp

<p>Medium (CVSS: 6.1) NVT: jQuery 1.0.3 < 3.5.0 XSS Vulnerability</p>
<p>Summary jQuery is prone to a cross-site scripting (XSS) vulnerability when appending HTML containing option elements.</p>
<p>Quality of Detection (QoD): 30%</p>
<p>Vulnerability Detection Result Installed version: 3.4.1 Fixed version: 3.5.0 Installation path / port: /cmn/js/lib/jquery-3.4.1.js Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info): - Identified file: https://10.0.0.1/cmn/js/lib/jquery-3.4.1.js - Referenced at: https://10.0.0.1/</p>
<p>Solution: Solution type: VendorFix Update to version 3.5.0 or later.</p>
<p>Affected Software/OS jQuery versions starting from 1.0.3 and prior to version 3.5.0.</p>
<p>Vulnerability Insight Passing HTML containing <option> elements from untrusted sources - even after sanitizing them - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: jQuery 1.0.3 < 3.5.0 XSS Vulnerability OID:1.3.6.1.4.1.25623.1.0.143813 Version used: 2025-01-31T15:39:24Z</p>
<p>References cve: CVE-2020-11023 cisa: Known Exploited Vulnerability (KEV) catalog url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog url: https://github.com/jquery/jquery/security/advisories/GHSA-jpcq-cgw6-v4j6 url: https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ url: https://masatokinugawa.10.cm/2020/05/jquery3.5.0-xss.html url: https://security.snyk.io/vuln/SNYK-JS-JQUERY-565129 cert-bund: WID-SEC-2024-3191 cert-bund: WID-SEC-2024-1872 cert-bund: WID-SEC-2023-0239</p>
<p>... continues on next page ...</p>

...continued from previous page ...	
cert-bund:	WID-SEC-2023-0063
cert-bund:	WID-SEC-2022-1347
cert-bund:	WID-SEC-2022-1189
cert-bund:	WID-SEC-2022-0757
cert-bund:	WID-SEC-2022-0732
cert-bund:	CB-K21/1085
cert-bund:	CB-K21/1067
cert-bund:	CB-K21/0418
cert-bund:	CB-K20/1049
cert-bund:	CB-K20/1027
cert-bund:	CB-K20/1025
cert-bund:	CB-K20/1024
cert-bund:	CB-K20/1021
cert-bund:	CB-K20/1008
cert-bund:	CB-K20/0870
cert-bund:	CB-K20/0800
cert-bund:	CB-K20/0705
cert-bund:	CB-K20/0521
dfn-cert:	DFN-CERT-2024-2743
dfn-cert:	DFN-CERT-2023-2027
dfn-cert:	DFN-CERT-2023-1197
dfn-cert:	DFN-CERT-2023-0481
dfn-cert:	DFN-CERT-2023-0245
dfn-cert:	DFN-CERT-2022-1988
dfn-cert:	DFN-CERT-2022-1610
dfn-cert:	DFN-CERT-2022-0119
dfn-cert:	DFN-CERT-2022-0074
dfn-cert:	DFN-CERT-2021-2348
dfn-cert:	DFN-CERT-2021-1687
dfn-cert:	DFN-CERT-2021-1111
dfn-cert:	DFN-CERT-2021-0820
dfn-cert:	DFN-CERT-2021-0633
dfn-cert:	DFN-CERT-2021-0563
dfn-cert:	DFN-CERT-2021-0545
dfn-cert:	DFN-CERT-2020-2776
dfn-cert:	DFN-CERT-2020-2423
dfn-cert:	DFN-CERT-2020-2335
dfn-cert:	DFN-CERT-2020-2287
dfn-cert:	DFN-CERT-2020-2227
dfn-cert:	DFN-CERT-2020-2209
dfn-cert:	DFN-CERT-2020-2074
dfn-cert:	DFN-CERT-2020-1743
dfn-cert:	DFN-CERT-2020-1712
dfn-cert:	DFN-CERT-2020-1509
dfn-cert:	DFN-CERT-2020-1506
dfn-cert:	DFN-CERT-2020-1433
dfn-cert:	DFN-CERT-2020-1163
...continues on next page ...	

...continued from previous page ...

dfn-cert: DFN-CERT-2020-1099

Medium (CVSS: 6.1)

NVT: jQuery 2.2.0 < 3.5.0 XSS Vulnerability

Summary

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

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 3.4.1

Fixed version: 3.5.0

Installation

path / port: /cmn/js/lib/jquery-3.4.1.js

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

- Identified file: <https://10.0.0.1/cmn/js/lib/jquery-3.4.1.js>
- Referenced at: <https://10.0.0.1/>

Impact

The flaw allows a remote attacker to execute arbitrary code via the <options> element.

Solution:**Solution type:** VendorFix

Update to version 3.5.0 or later.

Affected Software/OS

jQuery versions starting from 2.2.0 and prior to version 3.5.0.

Vulnerability Detection Method

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

Details: jQuery 2.2.0 < 3.5.0 XSS Vulnerability

OID:1.3.6.1.4.1.25623.1.0.104819

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

References

cve: CVE-2020-23064

url: <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>url: https://bugzilla.redhat.com/show_bug.cgi?id=2217733

cert-bund: WID-SEC-2023-1572

Medium (CVSS: 6.1)

NVT: jQuery 1.2 < 3.5.0 XSS Vulnerability

... continues on next page ...

...continued from previous page ...
Summary jQuery is prone to a cross-site scripting (XSS) vulnerability in jQuery.htmlPrefilter and related methods.
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 3.4.1 Fixed version: 3.5.0 Installation path / port: /cmn/js/lib/jquery-3.4.1.js Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info): - Identified file: https://10.0.0.1/cmn/js/lib/jquery-3.4.1.js - Referenced at: https://10.0.0.1/
Solution: Solution type: VendorFix Update to version 3.5.0 or later.
Affected Software/OS jQuery versions starting from 1.2 and prior to version 3.5.0.
Vulnerability Insight Passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: jQuery 1.2 < 3.5.0 XSS Vulnerability OID:1.3.6.1.4.1.25623.1.0.143812 Version used: 2023-07-14T05:06:08Z
References cve: CVE-2020-11022 url: https://github.com/jquery/jquery/security/advisories/GHSA-gxr4-xjj5-5px2 url: https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ url: https://masatokinugawa.10.cm/2020/05/jquery3.5.0-xss.html url: https://security.snyk.io/vuln/SNYK-JS-JQUERY-567880 cert-bund: WID-SEC-2024-3217 cert-bund: WID-SEC-2024-1872 cert-bund: WID-SEC-2023-0239 cert-bund: WID-SEC-2023-0063 cert-bund: WID-SEC-2022-1767 cert-bund: WID-SEC-2022-1347 cert-bund: WID-SEC-2022-0740 cert-bund: WID-SEC-2022-0732
... continues on next page ...

...continued from previous page ...

cert-bund: WID-SEC-2022-0624
 cert-bund: CB-K22/0463
 cert-bund: CB-K21/1085
 cert-bund: CB-K21/0071
 cert-bund: CB-K21/0070
 cert-bund: CB-K21/0069
 cert-bund: CB-K21/0067
 cert-bund: CB-K21/0061
 cert-bund: CB-K21/0059
 cert-bund: CB-K20/1049
 cert-bund: CB-K20/1030
 cert-bund: CB-K20/1027
 cert-bund: CB-K20/1025
 cert-bund: CB-K20/1023
 cert-bund: CB-K20/1008
 cert-bund: CB-K20/0870
 cert-bund: CB-K20/0800
 cert-bund: CB-K20/0705
 cert-bund: CB-K20/0521
 dfn-cert: DFN-CERT-2025-0041
 dfn-cert: DFN-CERT-2023-2027
 dfn-cert: DFN-CERT-2023-1197
 dfn-cert: DFN-CERT-2023-0481
 dfn-cert: DFN-CERT-2023-0245
 dfn-cert: DFN-CERT-2022-1988
 dfn-cert: DFN-CERT-2022-1670
 dfn-cert: DFN-CERT-2022-0869
 dfn-cert: DFN-CERT-2022-0074
 dfn-cert: DFN-CERT-2021-2190
 dfn-cert: DFN-CERT-2021-1111
 dfn-cert: DFN-CERT-2021-0828
 dfn-cert: DFN-CERT-2021-0826
 dfn-cert: DFN-CERT-2021-0819
 dfn-cert: DFN-CERT-2021-0633
 dfn-cert: DFN-CERT-2021-0545
 dfn-cert: DFN-CERT-2021-0140
 dfn-cert: DFN-CERT-2021-0138
 dfn-cert: DFN-CERT-2021-0135
 dfn-cert: DFN-CERT-2021-0132
 dfn-cert: DFN-CERT-2020-2423
 dfn-cert: DFN-CERT-2020-2335
 dfn-cert: DFN-CERT-2020-2305
 dfn-cert: DFN-CERT-2020-2286
 dfn-cert: DFN-CERT-2020-2227
 dfn-cert: DFN-CERT-2020-2209
 dfn-cert: DFN-CERT-2020-2130
 dfn-cert: DFN-CERT-2020-2074

...continues on next page ...

...continued from previous page ...
dfn-cert: DFN-CERT-2020-2015
dfn-cert: DFN-CERT-2020-2001
dfn-cert: DFN-CERT-2020-1838
dfn-cert: DFN-CERT-2020-1812
dfn-cert: DFN-CERT-2020-1712
dfn-cert: DFN-CERT-2020-1509
dfn-cert: DFN-CERT-2020-1506
dfn-cert: DFN-CERT-2020-1433
dfn-cert: DFN-CERT-2020-1163
dfn-cert: DFN-CERT-2020-1161
dfn-cert: DFN-CERT-2020-1138
dfn-cert: DFN-CERT-2020-1099

Medium (CVSS: 5.0) NVT: SSL/TLS: Certificate Expired
Product detection result cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25 ↪623.1.0.103692)
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 2025-01-07 23:59:59. Certificate details: fingerprint (SHA-1) BD8A1468752F2538F276866682062627085AAC99 fingerprint (SHA-256) 39F851C178CE325EF84773FB6777B8A64A2D165A5FE619 ↪B7F58E05A9FCE2DFC4 issued by CN=COMODO RSA Organization Validation Secure S ↪erver CA,O=COMODO CA Limited,L=Salford,ST=Greater Manchester,C=GB public key algorithm RSA public key size (bits) 2048 serial 5812E9A4279A45F95DD1FB8E896B6F12 signature algorithm sha256WithRSAEncryption subject CN=myrouter.io,O=Comcast Corporation,ST=Pennsy ↪lvania,C=US subject alternative names (SAN) myrouter.io valid from 2024-01-08 00:00:00 UTC valid until 2025-01-07 23:59:59 UTC
Solution: Solution type: Mitigation
... continues on next page ...

...continued from previous page ...
Replace the SSL/TLS certificate by a new one.
Vulnerability Insight This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.
Vulnerability Detection Method Details: SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: 2024-06-14T05:05:48Z
Product Detection Result Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Collect and Report Certificate Details OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 5.0) NVT: Backup File Scanner (HTTP) - Unreliable Detection Reporting
Summary The script reports backup files left on the web server.
Quality of Detection (QoD): 30%
Vulnerability Detection Result The following backup files were identified (<URL>:<Matching pattern>): https://10.0.0.1/cmn/css/.common-min.css.backup:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.common-min.css.bak:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.common-min.css.bkp:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.common-min.css.copy:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.common-min.css.old:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.common-min.css.orig:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.common-min.css.save:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.common-min.css.swp:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.common-min.css.temp:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.common-min.css.tmp:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.print.css.backup:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.print.css.bak:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.print.css.bkp:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.print.css.copy:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.print.css.old:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.print.css.orig:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.print.css.save:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.print.css.swp:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.print.css.temp:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/.print.css.tmp:~HTTP/1\.[01] 200
... continues on next page ...

...continued from previous page...

```

https://10.0.0.1/cmn/css/common-min.css.backup:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/common-min.css.bak:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/common-min.css.bkp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/common-min.css.copy:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/common-min.css.old:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/common-min.css.orig:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/common-min.css.save:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/common-min.css.swp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/common-min.css.temp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/common-min.css.tmp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.backup:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.bak:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.bkp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.copy:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.old:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.orig:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.save:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.swp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.temp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.tmp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.backup:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.bak:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.bkp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.copy:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.old:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.orig:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.save:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.swp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.temp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.tmp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.backup:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.bak:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.bkp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.copy:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.old:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.orig:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.save:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.swp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.temp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.tmp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.backup:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.bak:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.bkp:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.copy:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.old:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.orig:~HTTP/1\.[01] 200
https://10.0.0.1/cmn/css/lib/progressBar.css.save:~HTTP/1\.[01] 200

```

...continues on next page...

...continued from previous page ...
<pre> https://10.0.0.1/cmn/css/lib/progressBar.css.swp:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/lib/progressBar.css.temp:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/lib/progressBar.css.tmp:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/print.css.backup:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/print.css.bak:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/print.css.bkp:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/print.css.copy:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/print.css.old:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/print.css.orig:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/print.css.save:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/print.css.swp:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/print.css.temp:~HTTP/1\.[01] 200 https://10.0.0.1/cmn/css/print.css.tmp:~HTTP/1\.[01] 200 </pre>
<p>Impact</p> <p>Based on the information provided in these files an attacker might be able to gather sensitive information stored in these files.</p>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>Delete the backup files.</p>
<p>Vulnerability Insight</p> <p>Notes:</p> <ul style="list-style-type: none"> - 'Unreliable Detection' means that a file was detected only based on a HTTP 200 (Found) status code reported by the remote web server when a file was requested. - As the VT 'Backup File Scanner (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.140853) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.
<p>Vulnerability Detection Method</p> <p>Reports previous enumerated backup files accessible on the remote web server.</p> <p>Details: Backup File Scanner (HTTP) - Unreliable Detection Reporting</p> <p>OID:1.3.6.1.4.1.25623.1.0.108975</p> <p>Version used: 2022-09-13T10:15:09Z</p>
<p>References</p> <p>url: http://www.openwall.com/lists/oss-security/2017/10/31/1</p>
<p>Medium (CVSS: 4.0)</p> <p>NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability</p>
<p>Summary</p> <p>The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).</p>
<p>Quality of Detection (QoD): 80%</p>
... continues on next page ...

...continued from previous page ...
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

[\[return to 10.0.0.1 \]](#)

2.4.5 Medium 53/tcp

Medium (CVSS: 4.0) NVT: Dnsmasq < 2.85 DNS Cache Poisoning Vulnerability
Product detection result cpe:/a:thekelleys:dnsmasq:2.83 Detected by Dnsmasq Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.117275)
Summary Dnsmasq is prone to a DNS cache poisoning vulnerability. ... continues on next page ...

...continued from previous page ...
Quality of Detection (QoD): 30%
Vulnerability Detection Result Installed version: 2.83 Fixed version: 2.85 Installation path / port: 53/tcp
Solution: Solution type: VendorFix Update to version 2.85 or later.
Affected Software/OS Dnsmasq prior to 2.85.
Vulnerability Insight When configured to use a specific server for a given network interface, dnsmasq uses a fixed port while forwarding queries. An attacker on the network, able to find the outgoing port used by dnsmasq, only needs to guess the random transmission ID to forge a reply and get it accepted by dnsmasq. This flaw makes a DNS Cache Poisoning attack much easier. The highest threat from this vulnerability is to data integrity.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Dnsmasq < 2.85 DNS Cache Poisoning Vulnerability OID:1.3.6.1.4.1.25623.1.0.117321 Version used: 2021-08-27T08:01:04Z
Product Detection Result Product: cpe:/a:thekelleys:dnsmasq:2.83 Method: Dnsmasq Detection Consolidation OID: 1.3.6.1.4.1.25623.1.0.117275)
References cve: CVE-2021-3448 url: https://lists.thekelleys.org.uk/pipermail/dnsmasq-discuss/2021q2/014962.htm ↩1 url: https://bugzilla.redhat.com/show_bug.cgi?id=1939368 url: https://www.thekelleys.org.uk/dnsmasq/CHANGELOG cert-bund: WID-SEC-2022-1335 cert-bund: WID-SEC-2022-1329 cert-bund: WID-SEC-2022-1228 cert-bund: WID-SEC-2022-0624 dfn-cert: DFN-CERT-2022-1143
... continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2022-0906
 dfn-cert: DFN-CERT-2021-2246
 dfn-cert: DFN-CERT-2021-0720

[\[return to 10.0.0.1 \]](#)

2.4.6 Medium 80/tcp

Medium (CVSS: 6.1)

NVT: jQuery 2.2.0 < 3.5.0 XSS Vulnerability

Summary

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

Quality of Detection (QoD): 30%

Vulnerability Detection Result

Installed version: 3.4.1

Fixed version: 3.5.0

Installation

path / port: /cmn/js/lib/jquery-3.4.1.js

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

- Identified file: http://10.0.0.1/cmn/js/lib/jquery-3.4.1.js
- Referenced at: http://10.0.0.1/

Impact

The flaw allows a remote attacker to execute arbitrary code via the <options> element.

Solution:

Solution type: VendorFix

Update to version 3.5.0 or later.

Affected Software/OS

jQuery versions starting from 2.2.0 and prior to version 3.5.0.

Vulnerability Detection Method

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

Details: jQuery 2.2.0 < 3.5.0 XSS Vulnerability

OID:1.3.6.1.4.1.25623.1.0.104819

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

References

cve: CVE-2020-23064

url: https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

url: https://bugzilla.redhat.com/show_bug.cgi?id=2217733

... continues on next page ...

...continued from previous page ...	
cert-bund: WID-SEC-2023-1572	
Medium (CVSS: 6.1) NVT: jQuery 1.0.3 < 3.5.0 XSS Vulnerability	
Summary jQuery is prone to a cross-site scripting (XSS) vulnerability when appending HTML containing option elements.	
Quality of Detection (QoD): 30%	
Vulnerability Detection Result Installed version: 3.4.1 Fixed version: 3.5.0 Installation path / port: /cmn/js/lib/jquery-3.4.1.js Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info): - Identified file: http://10.0.0.1/cmn/js/lib/jquery-3.4.1.js - Referenced at: http://10.0.0.1/	
Solution: Solution type: VendorFix Update to version 3.5.0 or later.	
Affected Software/OS jQuery versions starting from 1.0.3 and prior to version 3.5.0.	
Vulnerability Insight Passing HTML containing <option> elements from untrusted sources - even after sanitizing them - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: jQuery 1.0.3 < 3.5.0 XSS Vulnerability OID:1.3.6.1.4.1.25623.1.0.143813 Version used: 2025-01-31T15:39:24Z	
References cve: CVE-2020-11023 cisa: Known Exploited Vulnerability (KEV) catalog url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog url: https://github.com/jquery/jquery/security/advisories/GHSA-jpcq-cgw6-v4j6 url: https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ url: https://masatokinugawa.10.cm/2020/05/jquery3.5.0-xss.html	
... continues on next page ...	

...continued from previous page...	
url:	https://security.snyk.io/vuln/SNYK-JS-JQUERY-565129
cert-bund:	WID-SEC-2024-3191
cert-bund:	WID-SEC-2024-1872
cert-bund:	WID-SEC-2023-0239
cert-bund:	WID-SEC-2023-0063
cert-bund:	WID-SEC-2022-1347
cert-bund:	WID-SEC-2022-1189
cert-bund:	WID-SEC-2022-0757
cert-bund:	WID-SEC-2022-0732
cert-bund:	CB-K21/1085
cert-bund:	CB-K21/1067
cert-bund:	CB-K21/0418
cert-bund:	CB-K20/1049
cert-bund:	CB-K20/1027
cert-bund:	CB-K20/1025
cert-bund:	CB-K20/1024
cert-bund:	CB-K20/1021
cert-bund:	CB-K20/1008
cert-bund:	CB-K20/0870
cert-bund:	CB-K20/0800
cert-bund:	CB-K20/0705
cert-bund:	CB-K20/0521
dfn-cert:	DFN-CERT-2024-2743
dfn-cert:	DFN-CERT-2023-2027
dfn-cert:	DFN-CERT-2023-1197
dfn-cert:	DFN-CERT-2023-0481
dfn-cert:	DFN-CERT-2023-0245
dfn-cert:	DFN-CERT-2022-1988
dfn-cert:	DFN-CERT-2022-1610
dfn-cert:	DFN-CERT-2022-0119
dfn-cert:	DFN-CERT-2022-0074
dfn-cert:	DFN-CERT-2021-2348
dfn-cert:	DFN-CERT-2021-1687
dfn-cert:	DFN-CERT-2021-1111
dfn-cert:	DFN-CERT-2021-0820
dfn-cert:	DFN-CERT-2021-0633
dfn-cert:	DFN-CERT-2021-0563
dfn-cert:	DFN-CERT-2021-0545
dfn-cert:	DFN-CERT-2020-2776
dfn-cert:	DFN-CERT-2020-2423
dfn-cert:	DFN-CERT-2020-2335
dfn-cert:	DFN-CERT-2020-2287
dfn-cert:	DFN-CERT-2020-2227
dfn-cert:	DFN-CERT-2020-2209
dfn-cert:	DFN-CERT-2020-2074
dfn-cert:	DFN-CERT-2020-1743
dfn-cert:	DFN-CERT-2020-1712
...continues on next page...	

...continued from previous page ...

dfn-cert: DFN-CERT-2020-1509
 dfn-cert: DFN-CERT-2020-1506
 dfn-cert: DFN-CERT-2020-1433
 dfn-cert: DFN-CERT-2020-1163
 dfn-cert: DFN-CERT-2020-1099

Medium (CVSS: 6.1)

NVT: jQuery 1.2 < 3.5.0 XSS Vulnerability

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability in jQuery.htmlPrefilter and related methods.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

Installed version: 3.4.1

Fixed version: 3.5.0

Installation

path / port: /cmn/js/lib/jquery-3.4.1.js

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

- Identified file: http://10.0.0.1/cmn/js/lib/jquery-3.4.1.js

- Referenced at: http://10.0.0.1/

Solution:**Solution type:** VendorFix

Update to version 3.5.0 or later.

Affected Software/OS

jQuery versions starting from 1.2 and prior to version 3.5.0.

Vulnerability Insight

Passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code.

Vulnerability Detection Method

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

Details: jQuery 1.2 < 3.5.0 XSS Vulnerability

OID:1.3.6.1.4.1.25623.1.0.143812

Version used: 2023-07-14T05:06:08Z

References

cve: CVE-2020-11022

url: <https://github.com/jquery/jquery/security/advisories/GHSA-gxr4-xjj5-5px2>url: <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>

... continues on next page ...

...continued from previous page...	
url:	https://masatokinugawa.10.cm/2020/05/jquery3.5.0-xss.html
url:	https://security.snyk.io/vuln/SNYK-JS-JQUERY-567880
cert-bund:	WID-SEC-2024-3217
cert-bund:	WID-SEC-2024-1872
cert-bund:	WID-SEC-2023-0239
cert-bund:	WID-SEC-2023-0063
cert-bund:	WID-SEC-2022-1767
cert-bund:	WID-SEC-2022-1347
cert-bund:	WID-SEC-2022-0740
cert-bund:	WID-SEC-2022-0732
cert-bund:	WID-SEC-2022-0624
cert-bund:	CB-K22/0463
cert-bund:	CB-K21/1085
cert-bund:	CB-K21/0071
cert-bund:	CB-K21/0070
cert-bund:	CB-K21/0069
cert-bund:	CB-K21/0067
cert-bund:	CB-K21/0061
cert-bund:	CB-K21/0059
cert-bund:	CB-K20/1049
cert-bund:	CB-K20/1030
cert-bund:	CB-K20/1027
cert-bund:	CB-K20/1025
cert-bund:	CB-K20/1023
cert-bund:	CB-K20/1008
cert-bund:	CB-K20/0870
cert-bund:	CB-K20/0800
cert-bund:	CB-K20/0705
cert-bund:	CB-K20/0521
dfn-cert:	DFN-CERT-2025-0041
dfn-cert:	DFN-CERT-2023-2027
dfn-cert:	DFN-CERT-2023-1197
dfn-cert:	DFN-CERT-2023-0481
dfn-cert:	DFN-CERT-2023-0245
dfn-cert:	DFN-CERT-2022-1988
dfn-cert:	DFN-CERT-2022-1670
dfn-cert:	DFN-CERT-2022-0869
dfn-cert:	DFN-CERT-2022-0074
dfn-cert:	DFN-CERT-2021-2190
dfn-cert:	DFN-CERT-2021-1111
dfn-cert:	DFN-CERT-2021-0828
dfn-cert:	DFN-CERT-2021-0826
dfn-cert:	DFN-CERT-2021-0819
dfn-cert:	DFN-CERT-2021-0633
dfn-cert:	DFN-CERT-2021-0545
dfn-cert:	DFN-CERT-2021-0140
dfn-cert:	DFN-CERT-2021-0138
...continues on next page...	

...continued from previous page ...

```

dfn-cert: DFN-CERT-2021-0135
dfn-cert: DFN-CERT-2021-0132
dfn-cert: DFN-CERT-2020-2423
dfn-cert: DFN-CERT-2020-2335
dfn-cert: DFN-CERT-2020-2305
dfn-cert: DFN-CERT-2020-2286
dfn-cert: DFN-CERT-2020-2227
dfn-cert: DFN-CERT-2020-2209
dfn-cert: DFN-CERT-2020-2130
dfn-cert: DFN-CERT-2020-2074
dfn-cert: DFN-CERT-2020-2015
dfn-cert: DFN-CERT-2020-2001
dfn-cert: DFN-CERT-2020-1838
dfn-cert: DFN-CERT-2020-1812
dfn-cert: DFN-CERT-2020-1712
dfn-cert: DFN-CERT-2020-1509
dfn-cert: DFN-CERT-2020-1506
dfn-cert: DFN-CERT-2020-1433
dfn-cert: DFN-CERT-2020-1163
dfn-cert: DFN-CERT-2020-1161
dfn-cert: DFN-CERT-2020-1138
dfn-cert: DFN-CERT-2020-1099

```

Medium (CVSS: 5.0)

NVT: Backup File Scanner (HTTP) - Unreliable Detection Reporting

Summary

The script reports backup files left on the web server.

Quality of Detection (QoD): 30%**Vulnerability Detection Result**

The following backup files were identified (<URL>:<Matching pattern>):

```

http://10.0.0.1/cmn/css/.common-min.css.backup:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.common-min.css.bak:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.common-min.css.bkp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.common-min.css.copy:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.common-min.css.old:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.common-min.css.orig:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.common-min.css.save:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.common-min.css.swp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.common-min.css.temp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.common-min.css.tmp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.print.css.backup:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.print.css.bak:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.print.css.bkp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.print.css.copy:~HTTP/1\.[01] 200

```

... continues on next page ...

...continued from previous page...

```

http://10.0.0.1/cmn/css/.print.css.old:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.print.css.orig:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.print.css.save:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.print.css.swp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.print.css.temp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/.print.css.tmp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/common-min.css.backup:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/common-min.css.bak:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/common-min.css.bkp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/common-min.css.copy:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/common-min.css.old:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/common-min.css.orig:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/common-min.css.save:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/common-min.css.swp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/common-min.css.temp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/common-min.css.tmp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.backup:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.bak:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.bkp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.copy:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.old:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.orig:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.save:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.swp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.temp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.tmp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/progressBar.css.backup:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/progressBar.css.bak:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/progressBar.css.bkp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/progressBar.css.copy:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/progressBar.css.old:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/progressBar.css.orig:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/progressBar.css.save:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/progressBar.css.swp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/progressBar.css.temp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/progressBar.css.tmp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.backup:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.bak:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.bkp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.copy:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.old:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.orig:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.save:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.swp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.temp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/jquery.radioswitch.css.tmp:~HTTP/1\.[01] 200
http://10.0.0.1/cmn/css/lib/progressBar.css.backup:~HTTP/1\.[01] 200

```

...continues on next page...

...continued from previous page...
<pre> http://10.0.0.1/cmn/css/lib/progressBar.css.bak:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/lib/progressBar.css.bkp:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/lib/progressBar.css.copy:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/lib/progressBar.css.old:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/lib/progressBar.css.orig:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/lib/progressBar.css.save:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/lib/progressBar.css.swp:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/lib/progressBar.css.temp:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/lib/progressBar.css.tmp:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/print.css.backup:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/print.css.bak:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/print.css.bkp:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/print.css.copy:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/print.css.old:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/print.css.orig:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/print.css.save:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/print.css.swp:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/print.css.temp:~HTTP/1\.[01] 200 http://10.0.0.1/cmn/css/print.css.tmp:~HTTP/1\.[01] 200 </pre>
<p>Impact</p> <p>Based on the information provided in these files an attacker might be able to gather sensitive information stored in these files.</p>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>Delete the backup files.</p>
<p>Vulnerability Insight</p> <p>Notes:</p> <ul style="list-style-type: none"> - 'Unreliable Detection' means that a file was detected only based on a HTTP 200 (Found) status code reported by the remote web server when a file was requested. - As the VT 'Backup File Scanner (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.140853) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.
<p>Vulnerability Detection Method</p> <p>Reports previous enumerated backup files accessible on the remote web server.</p> <p>Details: Backup File Scanner (HTTP) - Unreliable Detection Reporting</p> <p>OID:1.3.6.1.4.1.25623.1.0.108975</p> <p>Version used: 2022-09-13T10:15:09Z</p>
<p>References</p> <p>url: http://www.openwall.com/lists/oss-security/2017/10/31/1</p>

<p>Medium (CVSS: 4.8)</p> <p>NVT: Cleartext Transmission of Sensitive Information via HTTP</p>
<p>Summary</p> <p>The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.</p>
<p>Quality of Detection (QoD): 80%</p>
<p>Vulnerability Detection Result</p> <p>The following input fields were identified (URL:input name):</p> <p>http://10.0.0.1/:password</p>
<p>Impact</p> <p>An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.</p>
<p>Solution:</p> <p>Solution type: Workaround</p> <p>Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.</p>
<p>Affected Software/OS</p> <p>Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.</p>
<p>Vulnerability Detection Method</p> <p>Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.</p> <p>The script is currently checking the following:</p> <ul style="list-style-type: none"> - HTTP Basic Authentication (Basic Auth) - HTTP Forms (e.g. Login) with input field of type 'password' <p>Details: Cleartext Transmission of Sensitive Information via HTTP</p> <p>OID:1.3.6.1.4.1.25623.1.0.108440</p> <p>Version used: 2023-09-07T05:05:21Z</p>
<p>References</p> <p>url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management</p> <p>url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure</p> <p>url: https://cwe.mitre.org/data/definitions/319.html</p>

[\[return to 10.0.0.1 \]](#)

2.4.7 Low general/icmp

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

[\[return to 10.0.0.1 \]](#)

2.4.8 Low general/tcp

Low (CVSS: 2.6) NVT: TCP Timestamps Information Disclosure
Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.
Quality of Detection (QoD): 80%
Vulnerability Detection Result It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 1334711073 Packet 2: 1334712144
Impact A side effect of this feature is that the uptime of the remote host can sometimes be computed.
Solution: Solution type: Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
Affected Software/OS TCP implementations that implement RFC1323/RFC7323.
Vulnerability Insight The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
Vulnerability Detection Method Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP Timestamps Information Disclosure OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2023-12-15T16:10:08Z
References url: https://datatracker.ietf.org/doc/html/rfc1323 url: https://datatracker.ietf.org/doc/html/rfc7323 url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152 url: https://www.fortiguard.com/psirt/FG-IR-16-090

[\[return to 10.0.0.1 \]](#)

2.5 10.0.0.176

Host scan start Tue Mar 4 17:08:34 2025 UTC

Host scan end Tue Mar 4 21:49:46 2025 UTC

Service (Port)	Threat Level
general/tcp	Low

2.5.1 Low general/tcp

Low (CVSS: 2.6) NVT: TCP Timestamps Information Disclosure
Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.
Quality of Detection (QoD): 80%
Vulnerability Detection Result It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 620732974 Packet 2: 3654329798
Impact A side effect of this feature is that the uptime of the remote host can sometimes be computed.
Solution: Solution type: Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
Affected Software/OS TCP implementations that implement RFC1323/RFC7323.
Vulnerability Insight The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
... continues on next page ...

...continued from previous page ...

Vulnerability Detection Method

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

Details: TCP Timestamps Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.80091

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

References

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

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

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

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

[\[return to 10.0.0.176 \]](#)

2.6 10.0.0.175

Host scan start Tue Mar 4 17:00:24 2025 UTC

Host scan end Tue Mar 4 17:39:21 2025 UTC

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

2.6.1 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

Summary

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

It was detected that the host implements RFC1323/RFC7323.

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

Packet 1: 323268838

Packet 2: 323268946

Impact

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

... continues on next page ...

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

[\[return to 10.0.0.175 \]](#)

2.6.2 Low general/icmp

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

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

[\[return to 10.0.0.175 \]](#)

2.7 10.0.0.190

Host scan start Tue Mar 4 17:59:53 2025 UTC

Host scan end Tue Mar 4 18:04:03 2025 UTC

Service (Port)	Threat Level
general/icmp	Low

2.7.1 Low general/icmp

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

[\[return to 10.0.0.190 \]](#)

2.8 10.0.0.141

Host scan start Tue Mar 4 16:54:18 2025 UTC
 Host scan end Tue Mar 4 17:00:23 2025 UTC

Service (Port)	Threat Level
general/icmp	Low

2.8.1 Low general/icmp

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

...continued from previous page ...

References

cve: CVE-1999-0524

url: <https://datatracker.ietf.org/doc/html/rfc792>

url: <https://datatracker.ietf.org/doc/html/rfc2780>

cert-bund: CB-K15/1514

cert-bund: CB-K14/0632

dfn-cert: DFN-CERT-2014-0658

[[return to 10.0.0.141](#)]

This file was automatically generated.