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 "Scans ". The scan started at Tue Mar 4 16:53:21 2025 UTC and ended at Wed Mar 5 01:05:46 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

Host	High	Medium	Low	Log	False Positive
10.0.0.116	1	0	0	0	0
10.0.0.245	1	0	2	0	0
10.0.0.92	42	27	3	0	0
10.0.0.1	4	13	2	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: 7	48	40	11	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 99 results selected by the filtering described above. Before filtering there were 300 results.

1.1 Host Authentications

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

2 Results per Host

2.1 10.0.0.116

Host scan start	Tue Mar 4 16:54:53 2025 UTC
Host scan end	Tue Mar 4 18:02:25 2025 UTC

Service (Port)	Threat Level
443/tcp	High

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 10.0.0.116]

2.2 10.0.0.245

Host scan start Tue Mar 4 17:37:40 2025 UTC
Host scan end Tue Mar 4 19:19:09 2025 UTC

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

2.2.1 High 443/tcp

High (CVSS: 10.0) NVT: Greenbone Security Assistant (GSA) Default Credentials (HTTP)
Summary
. . . continues on next page . . .

... continued from previous page ...

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]

2.2.2 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:

... continues on next page ...

... continued from previous page ...

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]

2.2.3 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: 382054666
Packet 2: 382055728
```

Impact

... continues on next page ...

... continued from previous page ...

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/d`
`↪ownload/details.aspx?id=9152`
`url: https://www.fortiguard.com/psirt/FG-IR-16-090`

[return to 10.0.0.245]

2.3 10.0.0.92

Host scan start Tue Mar 4 16:54:53 2025 UTC
Host scan end Tue Mar 4 18:15:19 2025 UTC

Service (Port)	Threat Level
22/tcp	High
3128/tcp	High
53/tcp	High
80/tcp	High

... (continues) ...

... (continued) ...

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

2.3.1 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.

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.

... 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 8.9 - 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: 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:       22/tcp
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

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/releasenotes.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
```

... continues on next page ...

... continued from previous page ...

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 'regreSSHion'.

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.
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/regressh
↪ion-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: 7.5)
NVT: Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)

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

... continues on next page ...

... continued from previous page ...

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.

Quality of Detection (QoD): 30%

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
```

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.

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.

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.

... continues on next page ...

... continued from previous page ...

- 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.

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`

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-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_Se`
`↪curity_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`

... continues on next page ...

... 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]

2.3.2 High 3128/tcp

High (CVSS: 7.8)
NVT: Squid DoS Vulnerability (GHSA-jm7h-w5q5-jpq9, SQUID-2020:13)

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.
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.

... continues on next page ...

... continued from previous page ...

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-jpq`
`↪9`

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 ...

Due to an Uncontrolled Recursion bug, Squid may be vulnerable to a Denial of Service attack against HTTP Chunked decoder.
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'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Squid DoS Vulnerability (GHSA-72c2-c3wm-8qxc, SQUID-2024:1)`
OID:1.3.6.1.4.1.25623.1.0.114405
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-2024-25111
url: https://github.com/squid-cache/squid/security/advisories/GHSA-72c2-c3wm-8qx
↪c
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/chunked-stackoverflow.htm
↪l
cert-bund: WID-SEC-2024-0544
dfn-cert: DFN-CERT-2024-2191
dfn-cert: DFN-CERT-2024-1017
dfn-cert: DFN-CERT-2024-0956
dfn-cert: DFN-CERT-2024-0894
dfn-cert: DFN-CERT-2024-0797
dfn-cert: DFN-CERT-2024-0742
dfn-cert: DFN-CERT-2024-0642
```

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)
```

Summary
Squid is prone to multiple zero-day (0-day) vulnerabilities.

... continues on next page ...

... continued from previous page ...

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
- FTP Authentication Crash
- Assertion Crash In HTTP Response Headers Handling
- Implicit Assertion in Stream Handling

... continues on next page ...

... continued from previous page ...

Note: One GHSA advisory has been provided by the security researcher but is not published / available yet.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Squid Multiple 0-Day Vulnerabilities (Oct 2023)`
OID:1.3.6.1.4.1.25623.1.0.100439
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/`
`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`

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

... continues on next page ...

... continued from previous page ...

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'.

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-c6r
↪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 DoS Vulnerability (GHSA-8w9r-p88v-mmx9, SQUID-2023:7)

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 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-mmx
↪9
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
```

... continues on next page ...

... continued from previous page ...

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
Squid version 2.x and later prior to version 6.0.1.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Due to a NULL pointer dereference bug Squid is vulnerable to a Denial of Service attack against Squid's Gopher gateway.
The gopher protocol is always available and enabled in Squid prior to Squid 6.0.1.
Responses triggering this bug are possible to be received from any gopher server, even those without malicious intent.
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'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Squid DoS Vulnerability (GHSA-cg5h-v6vc-w33f, SQUID-2021:8)`
OID:1.3.6.1.4.1.25623.1.0.151071
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-2023-46728`
`url: https://github.com/squid-cache/squid/security/advisories/GHSA-cg5h-v6vc-w33f`
`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/gopher-nullpointer.html`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2023-2837`
`dfn-cert: DFN-CERT-2024-0970`
`dfn-cert: DFN-CERT-2024-0214`
`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-2023-2956`
`dfn-cert: DFN-CERT-2023-2934`

High (CVSS: 7.5)
NVT: Squid DoS Vulnerability (GHSA-h5x6-w8mv-xfpr, SQUID-2024:2)

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 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-xfp
↪r
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
```

... continues on next page ...

... continued from previous page ...

```
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-phqj-m8gv-cq4g, SQUID-2023:3)

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.

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

... continues on next page ...

... continued from previous page ...

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-cq4
↪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/digest-overflow.html
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2023-2725
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

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

... continues on next page ...

... continued from previous page ...

path / port: 3128/tcp

Solution:
Solution type: VendorFix
Update to version 6.0.1 or later.

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-q2g
↪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/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

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

... continues on next page ...

... continued from previous page ...

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)
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

... continues on next page ...

... continued from previous page ...

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-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
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.

... continues on next page ...

... continued from previous page ...

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-9329-3c2`
`↪7`
`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`
`dfn-cert: DFN-CERT-2024-0026`
`dfn-cert: DFN-CERT-2023-3192`
`dfn-cert: DFN-CERT-2023-3036`

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

... continues on next page ...

... continued from previous page ...

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.
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-g59
↪w
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

... continues on next page ...

... continued from previous page ...

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 Multiple DoS Vulnerabilities (GHSA-543m-w2m2-g255, SQUID-2023:2)

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 prior to 6.4.

Vulnerability Insight
The following flaws exist:
- 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

... continues on next page ...

... continued from previous page ...

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-g25
↪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 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
Fixed version: 7.0
Installation
path / port: 3128/tcp

Solution:

... continues on next page ...

... continued from previous page ...

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-q7h`
`↪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`
`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`

... continues on next page ...

... continued from previous page ...

```
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
```

[return to 10.0.0.92]

2.3.3 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
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.

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

[return to 10.0.0.92]

2.3.4 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

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

. . . continues on next page . . .

... continued from previous page ...

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 < 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: 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 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

... 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-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: 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:

... continues on next page ...

... continued from previous page ...

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`
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`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2380

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: 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

... continues on next page ...

... continued from previous page ...

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: 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
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`
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
. . . continues on next page . . .

... continued from previous page ...

```
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-argum
↪ent-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

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:       80/tcp
```

Solution:

... continues on next page ...

... continued from previous page ...

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`
`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: 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
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

. . . continues on next page . . .

... continued from previous page ...

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: 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:       80/tcp
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

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)

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`

... continues on next page ...

... continued from previous page ...

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
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:
- 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

... continues on next page ...

... continued from previous page ...

- 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`
`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: 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.

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 30%

Vulnerability Detection Result
Installed version: 2.4.52
Fixed version: 2.4.53
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
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

... continues on next page ...

... continued from previous page ...

```
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: 9.0)
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.

... continues on next page ...

... continued from previous page ...

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`
`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 < 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
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

... continues on next page ...

... continued from previous page ...

```
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
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:       80/tcp
```

Solution:

Solution type: VendorFix

Update to version 8.1.30, 8.2.24, 8.3.12 or later.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

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
- 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: 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:
- 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)

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

. . . continues on next page . . .

... continued from previous page ...

```
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-rjf4
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: 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

... continues on next page ...

... continued from previous page ...

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`

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%

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

```
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
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: 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

... continues on next page ...

... continued from previous page ...

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
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/bab0b99f376dac9170ac81382a5ed526938d5`
`↪95a`

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
```

... continues on next page ...

... continued from previous page ...

```
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 2.`
`↪..`
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
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: 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: 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

. . . continues on next page . . .

... continued from previous page ...

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: 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

... continues on next page ...

... continued from previous page ...

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: 7.0)
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)

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.

... continues on next page ...

... continued from previous page ...

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`
`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]

2.3.5 High 25/tcp

High (CVSS: 7.5)
NVT: Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)

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

Summary
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.

Quality of Detection (QoD): 30%

Vulnerability Detection Result
'DHE' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
'DHE' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
'DHE' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CCM
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_CCM
TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256

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.

Solution:
Solution type: Mitigation

. . . continues on next page . . .

... continued from previous page ...

- 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.

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.
- 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.

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`

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)

... continues on next page ...

... continued from previous page ...

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_Se
↪curity_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
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]

2.3.6 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
```

... continues on next page ...

... continued from previous page ...

Installation
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

... continues on next page ...

... continued from previous page ...

```
↪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
dfn-cert: DFN-CERT-2024-2602
dfn-cert: DFN-CERT-2024-2573
dfn-cert: DFN-CERT-2024-2392
```

... continues on next page ...

... continued from previous page ...

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
dfn-cert: DFN-CERT-2024-0597
dfn-cert: DFN-CERT-2024-0545
dfn-cert: DFN-CERT-2024-0526

... continues on next page ...

... continued from previous page ...

```
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: 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 possibl
↪e 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 < 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:       22/tcp
```

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/releasenotes.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:       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

... continues on next page ...

... continued from previous page ...

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/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:       22/tcp
```

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: 4.0)
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:       22/tcp
```

Solution:
Solution type: VendorFix

... 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]

2.3.7 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`

... continues on next page ...

... continued from previous page ...

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
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-w3p4-5cqh, 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.

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-w3p4-5cq

... continues on next page ...

... continued from previous page ...

```
↪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.

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.

... continues on next page ...

... continued from previous page ...

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
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]

2.3.8 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:

... continues on next page ...

... continued from previous page ...

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]

2.3.9 Medium 80/tcp

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:

... continues on next page ...

... continued from previous page ...

- 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`
`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: 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)`

... 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: 7.3.31
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
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: 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: 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

. . . continues on next page . . .

... continued from previous page ...

```
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
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.

... continues on next page ...

... continued from previous page ...

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 were 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.

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 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)

. . . continues on next page . . .

... continued from previous page ...

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: 5.5)
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

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: 80/tcp

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.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 8.0.22, 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
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

... continues on next page ...

... continued from previous page ...

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
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: phpinfo() Output Reporting (HTTP)

Summary

... continues on next page ...

... continued from previous page ...

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 potentiall
↪y 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)`
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
```

... continues on next page ...

... continued from previous page ...

cve: CVE-2023-49283
url: https://www.php.net/manual/en/function.phpinfo.php

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.

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

... continues on next page ...

... continued from previous page ...

```
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
dfn-cert: DFN-CERT-2021-2436
```

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 identi
↪fied:
http://10.0.0.92/mutillidae
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.

... continues on next page ...

... continued from previous page ...

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`

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: 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:      0000000000000000000000000000000000000000 cede8a534190bb52e7407197e53d424a7e0cbaf7 root <root@RIS430-Target.(none)> 1741032675 -0500
clone: from https://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
```

... continues on next page ...

... continued from previous page ...

```
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 reposit
↪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:      0000000000000000000000000000000000000000 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
Match:      DIRC
Used regex: ^DIRC
URL:        http://10.0.0.92/mutillidae/.git/index
Match:      Unnamed repository; edit this file 'description' to name the reposit
↪ory.
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

... continues on next page ...

... continued from previous page ...

Currently the script is checking for files/folders of the following SCM software:
- Git (.git)
- Mercurial (.hg)
- Bazaar (.bzr)
- 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: 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

... continues on next page ...

... continued from previous page ...

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: 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.

... continues on next page ...

... continued from previous page ...

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: 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)`

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

... continues on next page ...

... continued from previous page ...

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

[return to 10.0.0.92]

2.3.10 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'.
For Sendmail add the option 'O PrivacyOptions=goaway'.

... continues on next page ...

... continued from previous page ...

It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.

Vulnerability Insight
VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.

Vulnerability Detection Method
Details: `Check if Mailserver answer to VRFY and EXPN requests`
OID:1.3.6.1.4.1.25623.1.0.100072
Version used: `2023-10-31T05:06:37Z`

References
`url: http://cr.yp.to/smtp/vrfy.html`

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

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

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

Quality of Detection (QoD): 98%

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

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

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

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-09-27T05:05:23Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security:1.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

References
`cve: CVE-2011-3389`
`cve: CVE-2015-0204`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://datatracker.ietf.org/doc/rfc8996/`
`url: https://vnhacker.blogspot.com/2011/09/beast.html`
`url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1266`
`cert-bund: CB-K15/0850`
`cert-bund: CB-K15/0764`
`cert-bund: CB-K15/0720`
`cert-bund: CB-K15/0548`
`cert-bund: CB-K15/0526`
`cert-bund: CB-K15/0509`
`cert-bund: CB-K15/0493`
`cert-bund: CB-K15/0384`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156

... continues on next page ...

... continued from previous page ...

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

[return to 10.0.0.92]

2.3.11 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
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

. . . continues on next page . . .

... continued from previous page ...

```
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]

2.3.12 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: 1843670525
Packet 2: 1843671581
```

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`

... continues on next page ...

... continued from previous page ...

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/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090

[return to 10.0.0.92]

2.3.13 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

... continues on next page ...

... continued from previous page ...

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]

2.4 10.0.0.1

Host scan start Tue Mar 4 16:54:53 2025 UTC
Host scan end Tue Mar 4 21:23:05 2025 UTC

Service (Port)	Threat Level
53/tcp	High
443/tcp	High
12865/tcp	Medium
53/tcp	Medium
443/tcp	Medium
80/tcp	Medium
general/tcp	Low
general/icmp	Low

2.4.1 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%

... continues on next page ...

... continued from previous page ...

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.

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

... continues on next page ...

... continued from previous page ...

```
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
↪35.yaml
url: https://lists.thekelleys.org.uk/pipermail/dnsmasq-discuss/2022q1/016272.htm
↪l
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 < 2.90 Multiple DoS Vulnerabilities (KeyTrap)

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 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

... continues on next page ...

... continued from previous page ...

Update to version 2.90 or later.

Affected Software/OS
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`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2024-1223
dfn-cert: DFN-CERT-2024-1011
dfn-cert: DFN-CERT-2024-0984
dfn-cert: DFN-CERT-2024-0977
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
```

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

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Dnsmasq <= 2.89 UDP Fragmentation DoS Vulnerability
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:dnsmasq:2.83
Method: Dnsmasq 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=dnsmasq.git;a=commit;h=eb92fb32b746f210
↪4b0f370b5b295bb8dd4bd5e5
url: https://thekelleys.org.uk/dnsmasq/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

[return to 10.0.0.1]

2.4.2 High 443/tcp

High (CVSS: 7.5)
NVT: Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)

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

Summary
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.

Quality of Detection (QoD): 30%

Vulnerability Detection Result
'DHE' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

... continues on next page ...

... continued from previous page ...

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

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.

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.

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.
- 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.

... continues on next page ...

... continued from previous page ...

- 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.

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`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

References
`cve: CVE-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_Se`
`↪curity_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`
`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]

2.4.3 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 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.

Quality of Detection (QoD): 30%

Vulnerability Detection Result
`Installed version: 2.83`

. . . continues on next page . . .

... continued from previous page ...

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
↪l
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
dfn-cert: DFN-CERT-2022-0906
dfn-cert: DFN-CERT-2021-2246
dfn-cert: DFN-CERT-2021-0720

[return to 10.0.0.1]

2.4.5 Medium 443/tcp

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: 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 1.0.3 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.l0.cm/2020/05/jquery3.5.0-xss.html
url: https://security.snyk.io/vuln/SNYK-JS-JQUERY-565129
cert-bund: WID-SEC-2024-3191
```

... continues on next page ...

... continued from previous page ...

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
dfn-cert: DFN-CERT-2020-1509
dfn-cert: DFN-CERT-2020-1506

... continues on next page ...

... continued from previous page ...

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: 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.l0.cm/2020/05/jquery3.5.0-xss.html
url: https://security.snyk.io/vuln/SNYK-JS-JQUERY-567880

... continues on next page ...

... continued from previous page ...

```
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
dfn-cert: DFN-CERT-2021-0135
dfn-cert: DFN-CERT-2021-0132
```

... continues on next page ...

... continued from previous page ...

```
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: 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

... continues on next page ...

... continued from previous page ...

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: 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
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
```

... continues on next page ...

... continued from previous page ...

```
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
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
```

... continues on next page ...

... continued from previous page ...

```
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
```

Impact
Based on the information provided in these files an attacker might be able to gather sensitive information stored in these files.

Solution:
Solution type: Mitigation
Delete the backup files.

Vulnerability Insight
Notes:
- '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.

Vulnerability Detection Method
Reports previous enumerated backup files accessible on the remote web server.
Details: `Backup File Scanner (HTTP) - Unreliable Detection Reporting`
OID:1.3.6.1.4.1.25623.1.0.108975
Version used: `2022-09-13T10:15:09Z`

References
`url: http://www.openwall.com/lists/oss-security/2017/10/31/1`

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

... continues on next page ...

... continued from previous page ...

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
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: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

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

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Server Temporary Key Size: 1024 bits`

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

Solution:
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
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]

2.4.6 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%

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

```
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.l0.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
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
```

... continues on next page ...

... continued from previous page ...

```
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
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

... continues on next page ...

... continued from previous page ...

```
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/
url: https://masatokinugawa.l0.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
```

... continues on next page ...

... continued from previous page ...

```
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
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
```

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

```
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
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
```

... continues on next page ...

... continued from previous page ...

```
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
```

Impact
Based on the information provided in these files an attacker might be able to gather sensitive information stored in these files.

Solution:
Solution type: Mitigation
Delete the backup files.

Vulnerability Insight
Notes:
- '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.

Vulnerability Detection Method
Reports previous enumerated backup files accessible on the remote web server.
Details: `Backup File Scanner (HTTP) - Unreliable Detection Reporting`
OID:1.3.6.1.4.1.25623.1.0.108975
Version used: `2022-09-13T10:15:09Z`

References
`url: http://www.openwall.com/lists/oss-security/2017/10/31/1`

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The following input fields were identified (URL:input name):`
`http://10.0.0.1/:password`

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

References
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[return to 10.0.0.1]

2.4.7 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: 1334696047
Packet 2: 1334697099
```

Impact

... continues on next page ...

... continued from previous page ...

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/d`
`↪ownload/details.aspx?id=9152`
`url: https://www.fortiguard.com/psirt/FG-IR-16-090`

[return to 10.0.0.1]

2.4.8 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%

... continues on next page ...

... continued from previous page ...

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]

2.5 10.0.0.175

Host scan start	Tue Mar 4 17:00:51 2025 UTC
Host scan end	Tue Mar 4 17:32:44 2025 UTC

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

2.5.1 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
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 10.0.0.175]

2.5.2 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: 323271709
Packet 2: 323271817
```

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.

... continues on next page ...

... continued from previous page ...

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/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090

[return to 10.0.0.175]

2.6 10.0.0.190

Host scan start	Tue Mar 4 17:32:45 2025 UTC
Host scan end	Tue Mar 4 17:37:39 2025 UTC

Service (Port)	Threat Level
general/icmp	Low

2.6.1 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

... continues on next page ...

... continued from previous page ...

- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

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]

2.7 10.0.0.141

Host scan start	Tue Mar 4 16:54:53 2025 UTC
Host scan end	Tue Mar 4 17:01:01 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

... continues on next page ...

... continued from previous page ...

```
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 10.0.0.141]