Scan Report

June 9, 2022

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 "62a20330ce6e4a0040eaea2d-62a20330ce6e4a0040eaea36". The scan started at Thu Jun 9 14:27:47 2022 UTC and ended at Thu Jun 9 14:43:22 2022 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
13.58.47.204	51	46	5	17	0
Total: 1	51	46	5	17	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.

This report contains all 119 results selected by the filtering described above. Before filtering there were 119 results.

2 Results per Host

2.1 13.58.47.204

Host scan start	Thu Jun 9 14:28:43 2022 UTC
Host scan end	Thu Jun 9 14:43:11 2022 UTC

Service (Port)	Threat Level
80/tcp	High
80/tcp	Medium
general/tcp	Low
80/tcp	Low
general/CPE-T	Log
general/tcp	Log
80/tcp	Log

2.1.1 High 80/tcp

High (CVSS: 9.8)
NVT: Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Windows

Product detection result
`cpe:/a:apache:http_server:2.4.25`
`Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1`
`↪.0.117232)`

. . . continues on next page . . .

... continued from previous page ...

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 2.4.25`
`Fixed version: 2.4.48`
`Installation path / port: 80/tcp`

Impact
- CVE-2020-13938: This flaw lets unprivileged local users stop httpd on Windows.
- CVE-2020-35452: A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest.
- CVE-2021-26690: A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service.
- CVE-2021-26691: A specially crafted SessionHeader sent by an origin server could cause a heap overflow.

Solution:
Solution type: VendorFix
Update to version 2.4.48 or later.

Affected Software/OS
Apache HTTP Server versions 2.4.0 to 2.4.46 on Windows.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2020-13938: Improper Handling of Insufficient Privileges
- CVE-2020-35452: mod_auth_digest possible stack overflow by one null byte
- CVE-2021-26690: mod_session NULL pointer dereference
- CVE-2021-26691: mod_session response handling heap overflow

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.112896
Version used: `2021-08-24T09:01:06Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.25`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
`cve: CVE-2020-13938`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2020-35452
cve: CVE-2021-26690
cve: CVE-2021-26691
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K22/0072
cert-bund: CB-K21/1092
cert-bund: CB-K21/1090
cert-bund: CB-K21/0646
dfn-cert: DFN-CERT-2022-1047
dfn-cert: DFN-CERT-2022-0672
dfn-cert: DFN-CERT-2022-0207
dfn-cert: DFN-CERT-2022-0122
dfn-cert: DFN-CERT-2022-0098
dfn-cert: DFN-CERT-2021-2394
dfn-cert: DFN-CERT-2021-2365
dfn-cert: DFN-CERT-2021-2300
dfn-cert: DFN-CERT-2021-2187
dfn-cert: DFN-CERT-2021-2153
dfn-cert: DFN-CERT-2021-1467
dfn-cert: DFN-CERT-2021-1412
dfn-cert: DFN-CERT-2021-1355
dfn-cert: DFN-CERT-2021-1340
dfn-cert: DFN-CERT-2021-1333
dfn-cert: DFN-CERT-2021-1321
dfn-cert: DFN-CERT-2021-1317
dfn-cert: DFN-CERT-2021-1273
```

High (CVSS: 7.5)
NVT: Apache HTTP Server 2.4.17 < 2.4.49 'mod_proxy' HTTP/2 Request Smuggling Vulnerability - Windows

Product detection result

```
cpe:/a:apache:http_server:2.4.25
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 HTTP/2 request smuggling vulnerability in the 'mod_proxy' module.

Vulnerability Detection Result

```
Installed version: 2.4.25
Fixed version:     2.4.49
Installation
path / port:       80/tcp
```

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Update to version 2.4.49 or later.

Affected Software/OS
Apache HTTP Server version 2.4.17 through 2.4.48 running the mod_proxy module together with an enabled HTTP/2 protocol.

Vulnerability Insight
Apache's mod_proxy allows spaces in the :method of HTTP/2 requests, enabling request line injection. If the back-end server tolerates trailing junk in the request line, this lets an attacker to bypass block rules.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server 2.4.17 < 2.4.49 'mod_proxy' HTTP/2 Request Smuggling Vulnera.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.117616
Version used: `2021-09-17T11:59:51Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.25`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
`cve: CVE-2021-33193`
`url: https://portswigger.net/research/http2`
`url: https://github.com/apache/httpd/commit/ecebcc035ccd8d0e2984fe41420d9e944f45`
`↪6b3c`
`url: https://httpd.apache.org/security/vulnerabilities_24.html`
`cert-bund: CB-K21/0878`
`dfn-cert: DFN-CERT-2022-1047`
`dfn-cert: DFN-CERT-2021-2471`
`dfn-cert: DFN-CERT-2021-1961`
`dfn-cert: DFN-CERT-2021-1854`

High (CVSS: 7.5)
NVT: Apache HTTP Server 2.4.20 - 2.4.39 Multiple Vulnerabilities (Windows)

Product detection result
`cpe:/a:apache:http_server:2.4.25`
`Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1`
`↪.0.117232)`

... continues on next page ...

... continued from previous page ...

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 2.4.25
Fixed version: 2.4.41
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 2.4.41 or later.

Affected Software/OS
Apache HTTP Server version 2.4.20 to 2.4.39.

Vulnerability Insight
Apache HTTP server is prone to multiple vulnerabilities:
- A malicious client could perform a DoS attack by flooding a connection with requests and basically never reading responses on the TCP connection. Depending on h2 worker dimensioning, it was possible to block those with relatively few connections. (CVE-2019-9517)
- HTTP/2 very early pushes, for example configured with 'H2PushResource', could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client. (CVE-2019-10081)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server 2.4.20 - 2.4.39 Multiple Vulnerabilities (Windows)
OID:1.3.6.1.4.1.25623.1.0.114148
Version used: 2021-09-02T13:01:30Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2019-9517
cve: CVE-2019-10081
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K20/0708
cert-bund: CB-K19/0909
cert-bund: CB-K19/0728

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2021-0776
dfn-cert: DFN-CERT-2020-2422
dfn-cert: DFN-CERT-2020-0779
dfn-cert: DFN-CERT-2020-0716
dfn-cert: DFN-CERT-2020-0640
dfn-cert: DFN-CERT-2020-0630
dfn-cert: DFN-CERT-2020-0595
dfn-cert: DFN-CERT-2020-0054
dfn-cert: DFN-CERT-2019-2456
dfn-cert: DFN-CERT-2019-1992
dfn-cert: DFN-CERT-2019-1810
dfn-cert: DFN-CERT-2019-1751
dfn-cert: DFN-CERT-2019-1727
dfn-cert: DFN-CERT-2019-1690
```

High (CVSS: 7.5)
NVT: Apache HTTP Server 2.4.20 < 2.4.44 Multiple Vulnerabilities (Windows)

Product detection result

```
cpe:/a:apache:http_server:2.4.25
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.

Vulnerability Detection Result

```
Installed version: 2.4.25
Fixed version:     2.4.44
Installation
path / port:       80/tcp
```

Solution:

Solution type: VendorFix

Update to version 2.4.44 or later.

Affected Software/OS

Apache HTTP Server version 2.4.2 to 2.4.43.

Vulnerability Insight

The following vulnerabilities exist:

- Push Diary Crash on Specifically Crafted HTTP/2 Header (CVE-2020-9490)
- Push Diary Crash on Specifically Crafted HTTP/2 Header (CVE-2020-11993)

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server 2.4.20 < 2.4.44 Multiple Vulnerabilities (Windows)
OID:1.3.6.1.4.1.25623.1.0.144373
Version used: 2021-07-22T02:00:50Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2020-9490
cve: CVE-2020-11993
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K21/0341
cert-bund: CB-K21/0068
cert-bund: CB-K20/0798
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2021-1069
dfn-cert: DFN-CERT-2020-2628
dfn-cert: DFN-CERT-2020-2345
dfn-cert: DFN-CERT-2020-2338
dfn-cert: DFN-CERT-2020-1985
dfn-cert: DFN-CERT-2020-1905
dfn-cert: DFN-CERT-2020-1793
dfn-cert: DFN-CERT-2020-1744

High (CVSS: 7.5)
NVT: Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Windows)

Product detection result
cpe:/a:apache:http_server:2.4.25
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
In Apache HTTP Server mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

Vulnerability Detection Result
Installed version: 2.4.25
Fixed version: 2.4.38
Installation

... continues on next page ...

... continued from previous page ...

path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 2.4.38 or later.

Affected Software/OS
Apache HTTP Server version 2.4.37 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.141963
Version used: 2021-09-02T13:01:30Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2018-17199
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K19/0316
cert-bund: CB-K19/0071
dfn-cert: DFN-CERT-2021-1069
dfn-cert: DFN-CERT-2020-0673
dfn-cert: DFN-CERT-2019-2592
dfn-cert: DFN-CERT-2019-2456
dfn-cert: DFN-CERT-2019-0857
dfn-cert: DFN-CERT-2019-0690
dfn-cert: DFN-CERT-2019-0687
dfn-cert: DFN-CERT-2019-0198
dfn-cert: DFN-CERT-2019-0184

High (CVSS: 7.5)
NVT: Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Windows)

Product detection result
cpe:/a:apache:http_server:2.4.25
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

... continues on next page ...

... continued from previous page ...

Summary
In Apache HTTP Server, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

Vulnerability Detection Result
`Installed version: 2.4.25`
`Fixed version: 2.4.39`
`Installation path / port: 80/tcp`

Solution:
Solution type: VendorFix
Update to version 2.4.39 or later.

Affected Software/OS
Apache HTTP Server version 2.4.38 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability. ↪..`
OID:1.3.6.1.4.1.25623.1.0.142221
Version used: `2021-09-02T13:01:30Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.25`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
`cve: CVE-2019-0217`
`url: https://httpd.apache.org/security/vulnerabilities_24.html`
`cert-bund: CB-K19/0623`
`cert-bund: CB-K19/0267`
`dfn-cert: DFN-CERT-2019-2592`
`dfn-cert: DFN-CERT-2019-2456`
`dfn-cert: DFN-CERT-2019-0736`
`dfn-cert: DFN-CERT-2019-0690`
`dfn-cert: DFN-CERT-2019-0687`
`dfn-cert: DFN-CERT-2019-0680`
`dfn-cert: DFN-CERT-2019-0676`

High (CVSS: 7.5)
NVT: Apache HTTP Server < 2.4.48 NULL Pointer Dereference Vulnerability - Windows

Product detection result
cpe:/a:apache:http_server:2.4.25
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 NULL pointer dereference vulnerability.

Vulnerability Detection Result
Installed version: 2.4.25
Fixed version: 2.4.48
Installation
path / port: 80/tcp

Impact
Successful exploitation will allow an attacker to crash the server.

Solution:
Solution type: VendorFix
Update to version 2.4.48 or later.

Affected Software/OS
Apache HTTP Server before version 2.4.48 on Windows.

Vulnerability Insight
Apache HTTP Server protocol handler for the HTTP/2 protocol checks received request headers against the size limitations as configured for the server and used for the HTTP/1 protocol as well. On violation of these restrictions an HTTP response is sent to the client with a status code indicating why the request was rejected.
This rejection response was not fully initialised in the HTTP/2 protocol handler if the offending header was the very first one received or appeared in a footer. This led to a NULL pointer dereference on initialised memory, crashing reliably the child process.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server < 2.4.48 NULL Pointer Dereference Vulnerability - Windows
OID:1.3.6.1.4.1.25623.1.0.112904
Version used: 2021-08-24T09:01:06Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
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-2021-31618
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K21/0611
dfn-cert: DFN-CERT-2021-1549
dfn-cert: DFN-CERT-2021-1467
dfn-cert: DFN-CERT-2021-1355
dfn-cert: DFN-CERT-2021-1333
dfn-cert: DFN-CERT-2021-1329
dfn-cert: DFN-CERT-2021-1276
dfn-cert: DFN-CERT-2021-1273

High (CVSS: 9.8)
NVT: Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Windows

Product detection result

cpe:/a:apache:http_server:2.4.25
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.

Vulnerability Detection Result

Installed version: 2.4.25
Fixed version: 2.4.49
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 2.4.49 or later.

Affected Software/OS

Apache HTTP Server version 2.4.48 and prior.

Vulnerability Insight

The following vulnerabilities exist:
- CVE-2021-34798: NULL pointer dereference in httpd core
- CVE-2021-39275: ap_escape_quotes buffer overflow
- CVE-2021-40438: mod_proxy SSRF

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.146726
Version used: 2021-09-29T08:01:30Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2021-34798
cve: CVE-2021-39275
cve: CVE-2021-40438
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K22/0476
cert-bund: CB-K22/0465
cert-bund: CB-K22/0463
cert-bund: CB-K21/0992
dfn-cert: DFN-CERT-2022-0904
dfn-cert: DFN-CERT-2022-0878
dfn-cert: DFN-CERT-2022-0872
dfn-cert: DFN-CERT-2022-0869
dfn-cert: DFN-CERT-2022-0672
dfn-cert: DFN-CERT-2022-0207
dfn-cert: DFN-CERT-2022-0119
dfn-cert: DFN-CERT-2022-0098
dfn-cert: DFN-CERT-2021-2629
dfn-cert: DFN-CERT-2021-2471
dfn-cert: DFN-CERT-2021-2185
dfn-cert: DFN-CERT-2021-2164
dfn-cert: DFN-CERT-2021-2153
dfn-cert: DFN-CERT-2021-2098
dfn-cert: DFN-CERT-2021-2090
dfn-cert: DFN-CERT-2021-2047
dfn-cert: DFN-CERT-2021-2020
dfn-cert: DFN-CERT-2021-1961

High (CVSS: 9.8)
NVT: Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Windows

Product detection result
cpe:/a:apache:http_server:2.4.25
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1

... continues on next page ...

... continued from previous page ...

↪.0.117232)

Summary
Apache HTTP Server is prone to a buffer overflow vulnerability.

Vulnerability Detection Result
Installed version: 2.4.25
Fixed version: 2.4.52
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 2.4.52 or later.

Affected Software/OS
Apache HTTP Server versions through 2.4.51.

Vulnerability Insight
A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Windows
OID:1.3.6.1.4.1.25623.1.0.117857
Version used: 2021-12-23T12:12:57Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2021-44790
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K22/0619
cert-bund: CB-K21/1296
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-0747
dfn-cert: DFN-CERT-2022-0369
dfn-cert: DFN-CERT-2022-0192

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-0098
dfn-cert: DFN-CERT-2022-0068
dfn-cert: DFN-CERT-2021-2656

High (CVSS: 9.8)
NVT: Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Windows

Product detection result
cpe:/a:apache:http_server:2.4.25
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.

Vulnerability Detection Result
Installed version: 2.4.25
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 - Windows
OID:1.3.6.1.4.1.25623.1.0.113838
Version used: 2022-03-21T03:03:41Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
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-2022-22719
cve: CVE-2022-22720
cve: CVE-2022-22721
cve: CVE-2022-23943
url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.53
cert-bund: CB-K22/0619
cert-bund: CB-K22/0306
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: 8.2)
NVT: Apache HTTP Server 2.4.7 - 2.4.51 Multiple Vulnerabilities - Windows

Product detection result

cpe:/a:apache:http_server:2.4.25
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.

Vulnerability Detection Result

Installed version: 2.4.25
Fixed version: 2.4.52
Installation
path / port: 80/tcp

Solution:

Solution type: VendorFix
Update to version 2.4.52 or later.

Affected Software/OS

Apache HTTP Server version 2.4.7 through 2.4.51.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server 2.4.7 - 2.4.51 Multiple Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.117855
Version used: `2021-12-23T12:12:57Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.25`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
`cve: CVE-2021-44224`
`url: https://httpd.apache.org/security/vulnerabilities_24.html`
`cert-bund: CB-K22/0619`
`cert-bund: CB-K21/1296`
`dfn-cert: DFN-CERT-2022-1116`
`dfn-cert: DFN-CERT-2022-1115`
`dfn-cert: DFN-CERT-2022-1114`
`dfn-cert: DFN-CERT-2022-1047`
`dfn-cert: DFN-CERT-2022-0872`
`dfn-cert: DFN-CERT-2022-0068`
`dfn-cert: DFN-CERT-2021-2656`

High (CVSS: 7.5)
NVT: Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Windows)

Product detection result
`cpe:/a:apache:http_server:2.4.25`
`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 vulnerability.

Vulnerability Detection Result
`Installed version: 2.4.25`
`Fixed version:     2.4.30`

... continues on next page ...

... continued from previous page ...

Installation
path / port: 80/tcp

Impact
Successful exploitation will allow an attacker to crash the Apache HTTP Server resulting in denial of service condition.

Solution:
Solution type: VendorFix
Update to version 2.4.30 or later. Please see the references for more information.

Affected Software/OS
Apache HTTP Server versions 2.4.6, 2.4.7, 2.4.9, 2.4.10, 2.4.12, 2.4.16 through 2.4.18, 2.4.20, 2.4.23, and 2.4.25 through 2.4.29.

Vulnerability Insight
The flaw exists as the Apache HTTP Server fails to sanitize against a specially crafted HTTP request header.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Windows)
OID:1.3.6.1.4.1.25623.1.0.812847
Version used: 2022-04-13T07:21:45Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2018-1303
url: https://httpd.apache.org/security/vulnerabilities_24.html
url: http://www.securityfocus.com/bid/103522
cert-bund: CB-K20/1030
cert-bund: CB-K18/0535
dfn-cert: DFN-CERT-2020-2133
dfn-cert: DFN-CERT-2019-0359
dfn-cert: DFN-CERT-2019-0351
dfn-cert: DFN-CERT-2018-2316
dfn-cert: DFN-CERT-2018-0985
dfn-cert: DFN-CERT-2018-0570

High (CVSS: 7.5)
NVT: Apache HTTP Server Denial-Of-Service Vulnerability June17 (Windows)

Product detection result
cpe:/a:apache:http_server:2.4.25
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 vulnerability.

Vulnerability Detection Result
Installed version: 2.4.25
Fixed version: 2.4.26
Installation
path / port: 80/tcp

Impact
Successful exploitation will allow remote attackers to cause a denial-of-service condition.

Solution:
Solution type: VendorFix
Update to Apache HTTP Server 2.2.33 or 2.4.26 or later.

Affected Software/OS
Apache HTTP Server versions 2.2.32, 2.4.24 and 2.4.25.

Vulnerability Insight
The flaw exists due to an error in the token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server Denial-Of-Service Vulnerability June17 (Windows)
OID:1.3.6.1.4.1.25623.1.0.811215
Version used: 2022-04-22T13:00:36Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2017-7668
url: http://seclists.org/oss-sec/2017/q2/510
url: http://www.securityfocus.com/bid/99137
url: http://httpd.apache.org/security/vulnerabilities_22.html
url: http://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K18/0066
cert-bund: CB-K17/2013
cert-bund: CB-K17/1936
cert-bund: CB-K17/1854
cert-bund: CB-K17/1842
cert-bund: CB-K17/1747
cert-bund: CB-K17/1622
cert-bund: CB-K17/1382
cert-bund: CB-K17/1279
cert-bund: CB-K17/1163
cert-bund: CB-K17/1023
dfn-cert: DFN-CERT-2019-0358
dfn-cert: DFN-CERT-2018-0077
dfn-cert: DFN-CERT-2017-2104
dfn-cert: DFN-CERT-2017-2021
dfn-cert: DFN-CERT-2017-1926
dfn-cert: DFN-CERT-2017-1925
dfn-cert: DFN-CERT-2017-1828
dfn-cert: DFN-CERT-2017-1692
dfn-cert: DFN-CERT-2017-1443
dfn-cert: DFN-CERT-2017-1327
dfn-cert: DFN-CERT-2017-1204
dfn-cert: DFN-CERT-2017-1058
```

High (CVSS: 7.5)
NVT: Apache HTTP Server 'HTTP/2 connection' DoS Vulnerability

Product detection result

```
cpe:/a:apache:http_server:2.4.25
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 vulnerability.

Vulnerability Detection Result

```
Installed version: 2.4.25
Fixed version:     2.4.34
Installation
path / port:       80/tcp
```

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow remote attackers to cause a denial of service (DoS) condition on a targeted system.

Solution:
Solution type: VendorFix
Update to Apache HTTP Server 2.4.34 or later. Please see the references for more information.

Affected Software/OS
Apache HTTP Server versions 2.4.18 through 2.4.30 and 2.4.33.

Vulnerability Insight
The flaw is due to an error in the handling of specially crafted HTTP/2 requests.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server 'HTTP/2 connection' DoS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.813812
Version used: `2021-06-15T02:00:29Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.25`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
`cve: CVE-2018-1333`
`url: http://seclists.org/oss-sec/2018/q3/39`
`url: https://httpd.apache.org/security/vulnerabilities_24.html`
`cert-bund: CB-K18/0805`
`dfn-cert: DFN-CERT-2019-0359`
`dfn-cert: DFN-CERT-2019-0351`
`dfn-cert: DFN-CERT-2018-2316`
`dfn-cert: DFN-CERT-2018-2011`
`dfn-cert: DFN-CERT-2018-1642`
`dfn-cert: DFN-CERT-2018-1412`

High (CVSS: 9.1)
NVT: Apache HTTP Server Memory Access Vulnerability (Windows)

Product detection result
`cpe:/a:apache:http_server:2.4.25`
`Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1`
`↪.0.117232)`

... continues on next page ...

... continued from previous page ...

Summary
Apache HTTP Server is prone to a memory access vulnerability.

Vulnerability Detection Result
Installed version: 2.4.25
Fixed version: 2.4.41
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 2.4.41 or later.

Affected Software/OS
Apache HTTP Server version 2.4.18 to 2.4.39.

Vulnerability Insight
Using fuzzed network input, the http/2 session handling could be made to read memory after being freed during connection shutdown.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server Memory Access Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.114150
Version used: 2021-09-02T13:01:30Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2019-10082
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K20/0708
cert-bund: CB-K19/0909
cert-bund: CB-K19/0728
dfn-cert: DFN-CERT-2020-2422
dfn-cert: DFN-CERT-2020-0716
dfn-cert: DFN-CERT-2019-1810
dfn-cert: DFN-CERT-2019-1751

High (CVSS: 9.1)
NVT: Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Windows)

Product detection result
cpe:/a:apache:http_server:2.4.25
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.

Vulnerability Detection Result
Installed version: 2.4.25
Fixed version: 2.4.27
Installation
path / port: 80/tcp

Impact
Successful exploitation will allow remote attackers to cause the target service to crash. A remote user can obtain potentially sensitive information as well on the target system.

Solution:
Solution type: VendorFix
Update to Apache HTTP Server 2.2.34 or 2.4.27 or later.

Affected Software/OS
Apache HTTP Server 2.2.x before 2.2.34 and 2.4.x before 2.4.27.

Vulnerability Insight
The flaw exists due to error in Apache 'mod_auth_digest' which does not properly initialize memory used to process 'Digest' type HTTP Authorization headers.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Windows)
OID:1.3.6.1.4.1.25623.1.0.811236
Version used: 2022-04-13T11:57:07Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2017-9788

. . . continues on next page . . .

... continued from previous page ...

```
url: http://www.securitytracker.com/id/1038906
url: http://www.securityfocus.com/bid/99569
url: http://httpd.apache.org/security/vulnerabilities_22.html
url: http://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K18/0066
cert-bund: CB-K17/2013
cert-bund: CB-K17/1980
cert-bund: CB-K17/1936
cert-bund: CB-K17/1871
cert-bund: CB-K17/1854
cert-bund: CB-K17/1842
cert-bund: CB-K17/1768
cert-bund: CB-K17/1747
cert-bund: CB-K17/1622
cert-bund: CB-K17/1558
cert-bund: CB-K17/1382
cert-bund: CB-K17/1197
cert-bund: CB-K17/1177
cert-bund: CB-K17/1023
dfn-cert: DFN-CERT-2019-0358
dfn-cert: DFN-CERT-2018-0077
dfn-cert: DFN-CERT-2017-2104
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-2021
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1926
dfn-cert: DFN-CERT-2017-1925
dfn-cert: DFN-CERT-2017-1843
dfn-cert: DFN-CERT-2017-1828
dfn-cert: DFN-CERT-2017-1692
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1443
dfn-cert: DFN-CERT-2017-1240
dfn-cert: DFN-CERT-2017-1217
dfn-cert: DFN-CERT-2017-1058
```

High (CVSS: 7.5)
NVT: Apache HTTP Server 'mod_http2' null pointer dereference DoS Vulnerability (Windows)

Product detection result

```
cpe:/a:apache:http_server:2.4.25
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 vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 2.4.25
Fixed version: 2.4.26
Installation
path / port: 80/tcp

Impact
Successful exploitation will allow remote attackers to cause a denial-of-service condition.

Solution:
Solution type: VendorFix
Update to Apache HTTP Server 2.4.26 or later.

Affected Software/OS
Apache HTTP Server version 2.4.25.

Vulnerability Insight
The flaw exists as a maliciously constructed HTTP/2 request could cause mod_http2 to dereference a NULL pointer and crash the server process.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server 'mod_http2' null pointer dereference DoS Vulnerability (Wind.
↪..
OID:1.3.6.1.4.1.25623.1.0.811217
Version used: 2022-04-13T11:57:07Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2017-7659
url: http://seclists.org/oss-sec/2017/q2/504
url: http://www.securityfocus.com/bid/99132
url: http://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K18/0187
cert-bund: CB-K17/1854
cert-bund: CB-K17/1622
cert-bund: CB-K17/1382
cert-bund: CB-K17/1023
dfn-cert: DFN-CERT-2019-0358
dfn-cert: DFN-CERT-2018-0206

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-1925
dfn-cert: DFN-CERT-2017-1692
dfn-cert: DFN-CERT-2017-1443
dfn-cert: DFN-CERT-2017-1058
```

High (CVSS: 9.8)
NVT: Apache HTTP Server Multiple Vulnerabilities Apr18 (Windows)

Product detection result

```
cpe:/a:apache:http_server:2.4.25
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.

Vulnerability Detection Result

```
Installed version: 2.4.25
Fixed version:     2.4.30
Installation
path / port:       80/tcp
```

Impact

Successful exploitation will allow an attacker to replay HTTP requests across servers without detection, influence the user content, upload a malicious file, crash the Apache HTTP Server and perform denial of service attack.

Solution:

Solution type: VendorFix

Update to version 2.4.30 or later. Please see the references for more information.

Affected Software/OS

Apache HTTP Server versions from 2.4.1 to 2.4.4, 2.4.6, 2.4.7, 2.4.9, 2.4.10, 2.4.12, 2.4.16 to 2.4.18, 2.4.20, 2.4.23, 2.4.25 to 2.4.29.

Vulnerability Insight

Multiple flaws exist due to:
- Apache HTTP Server fails to correctly generate the nonce sent to prevent reply attacks.
- Misconfigured mod_session variable, HTTP_SESSION.
- Apache HTTP Server fails to sanitize the expression specified in '<FilesMatch>'.
- An error in Apache HTTP Server 'mod_authnz_ldap' when configured with AuthLDAPCharsetConfig.
- Apache HTTP Server fails to sanitize against a specially crafted request.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server Multiple Vulnerabilities Apr18 (Windows)
OID:1.3.6.1.4.1.25623.1.0.812846
Version used: 2022-04-13T07:21:45Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2018-1312
cve: CVE-2018-1283
cve: CVE-2017-15715
cve: CVE-2017-15710
cve: CVE-2018-1301
url: https://httpd.apache.org/security/vulnerabilities_24.html
url: http://www.securityfocus.com/bid/103524
url: http://www.securityfocus.com/bid/103520
url: http://www.securityfocus.com/bid/103525
url: http://www.securityfocus.com/bid/103512
url: http://www.securityfocus.com/bid/103515
cert-bund: CB-K20/1030
cert-bund: CB-K19/0354
cert-bund: CB-K18/0535
dfn-cert: DFN-CERT-2020-2133
dfn-cert: DFN-CERT-2020-0673
dfn-cert: DFN-CERT-2019-1550
dfn-cert: DFN-CERT-2019-0736
dfn-cert: DFN-CERT-2019-0359
dfn-cert: DFN-CERT-2019-0351
dfn-cert: DFN-CERT-2018-2316
dfn-cert: DFN-CERT-2018-0985
dfn-cert: DFN-CERT-2018-0795
dfn-cert: DFN-CERT-2018-0703
dfn-cert: DFN-CERT-2018-0570

High (CVSS: 9.8)
NVT: Apache HTTP Server Multiple Vulnerabilities June17 (Windows)

Product detection result
cpe:/a:apache:http_server:2.4.25
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

... continues on next page ...

... continued from previous page ...

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 2.4.25`
`Fixed version: 2.4.26`
`Installation path / port: 80/tcp`

Impact
Successful exploitation will allow remote attackers to bypass authentication and perform unauthorized actions, cause a denial-of-service condition and gain access to potentially sensitive information.

Solution:
Solution type: VendorFix
Update to Apache HTTP Server 2.2.33 or 2.4.26 or later.

Affected Software/OS
Apache HTTP Server 2.2.x before 2.2.33 and 2.4.x before 2.4.26.

Vulnerability Insight
Multiple flaws exist as,
- The mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
- The mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
- An use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server Multiple Vulnerabilities June17 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.811213
Version used: `2022-04-13T11:57:07Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.25`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
`cve: CVE-2017-7679`
`cve: CVE-2017-3169`

... continues on next page ...

... continued from previous page ...

cve: CVE-2017-3167
url: http://seclists.org/oss-sec/2017/q2/509
url: http://www.securityfocus.com/bid/99135
url: http://www.securityfocus.com/bid/99134
url: http://httpd.apache.org/security/vulnerabilities_24.html
url: http://httpd.apache.org/security/vulnerabilities_22.html
cert-bund: CB-K22/0045
cert-bund: CB-K18/0066
cert-bund: CB-K17/2188
cert-bund: CB-K17/2013
cert-bund: CB-K17/1936
cert-bund: CB-K17/1854
cert-bund: CB-K17/1842
cert-bund: CB-K17/1768
cert-bund: CB-K17/1747
cert-bund: CB-K17/1622
cert-bund: CB-K17/1382
cert-bund: CB-K17/1279
cert-bund: CB-K17/1154
cert-bund: CB-K17/1023
dfn-cert: DFN-CERT-2019-0358
dfn-cert: DFN-CERT-2018-0077
dfn-cert: DFN-CERT-2017-2290
dfn-cert: DFN-CERT-2017-2104
dfn-cert: DFN-CERT-2017-2021
dfn-cert: DFN-CERT-2017-1926
dfn-cert: DFN-CERT-2017-1925
dfn-cert: DFN-CERT-2017-1843
dfn-cert: DFN-CERT-2017-1828
dfn-cert: DFN-CERT-2017-1692
dfn-cert: DFN-CERT-2017-1443
dfn-cert: DFN-CERT-2017-1327
dfn-cert: DFN-CERT-2017-1193
dfn-cert: DFN-CERT-2017-1058

High (CVSS: 7.5)
NVT: Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed) - Version Check

Product detection result
cpe:/a:apache:http_server:2.4.25
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary

... continues on next page ...

... continued from previous page ...

Apache HTTP Server allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed.

Vulnerability Detection Result
Installed version: 2.4.25
Fixed version: 2.4.28
Installation
path / port: 80/tcp

Impact
The successful exploitation allows the attacker to read chunks of the host's memory.

Solution:
Solution type: VendorFix
Update to Apache HTTP Server 2.4.28. For Apache HTTP Server running version 2.2.34 apply the patch linked in the references.
As a workaround the usage of .htaccess should be disabled competely via the 'AllowOverride None' directive within the webservers configuration. Furthermore all <Limit> statements within the webserver configuration needs to be verified for invalid HTTP methods.

Affected Software/OS
Apache HTTP Server 2.2.x versions up to 2.2.34 and 2.4.x below 2.4.28.

Vulnerability Insight
Optionsbleed is a use after free error in the Apache HTTP Server that causes a corrupted Allow header to be constructed in response to HTTP OPTIONS requests. This can leak pieces of arbitrary memory from the server process that may contain secrets. The memory pieces change after multiple requests, so for a vulnerable host an arbitrary number of memory chunks can be leaked.
The bug appears if a webmaster tries to use the 'Limit' directive with an invalid HTTP method.
Example .htaccess:
<Limit abcxyz> </Limit>

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed) - Version C.
↪..
OID:1.3.6.1.4.1.25623.1.0.108252
Version used: 2022-04-13T11:57:07Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

... continues on next page ...

... continued from previous page ...

References

cve: CVE-2017-9798
url: http://openwall.com/lists/oss-security/2017/09/18/2
url: https://blog.fuzzing-project.org/60-Optionsbleed-HTTP-OPTIONS-method-can-le
↪ak-Apaches-server-memory.html
url: http://www.securityfocus.com/bid/100872
url: https://archive.apache.org/dist/httpd/patches/apply_to_2.2.34/
url: https://www.apache.org/dist/httpd/CHANGES_2.4.28
cert-bund: CB-K18/1012
cert-bund: CB-K18/0800
cert-bund: CB-K18/0606
cert-bund: CB-K18/0098
cert-bund: CB-K18/0066
cert-bund: CB-K17/2188
cert-bund: CB-K17/2117
cert-bund: CB-K17/2021
cert-bund: CB-K17/1980
cert-bund: CB-K17/1936
cert-bund: CB-K17/1871
cert-bund: CB-K17/1773
cert-bund: CB-K17/1768
cert-bund: CB-K17/1587
dfn-cert: DFN-CERT-2019-0359
dfn-cert: DFN-CERT-2018-2113
dfn-cert: DFN-CERT-2018-1070
dfn-cert: DFN-CERT-2018-0725
dfn-cert: DFN-CERT-2018-0100
dfn-cert: DFN-CERT-2018-0077
dfn-cert: DFN-CERT-2017-2290
dfn-cert: DFN-CERT-2017-2211
dfn-cert: DFN-CERT-2017-2108
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-2021
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1854
dfn-cert: DFN-CERT-2017-1843
dfn-cert: DFN-CERT-2017-1659

High (CVSS: 9.9)
NVT: jQuery End of Life (EOL) Detection (Windows)

Summary

The installed version of jQuery on the remote host has reached the End of Life (EOL) and should not be used anymore.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
The "jQuery" version on the remote host has reached the end of life.
CPE:                cpe:/a:jquery:jquery:1.10.2
Installed version:  1.10.2
Location/URL:       http://13.58.47.204//code.jquery.com
EOL version:        1
EOL date:           unknown
```

Impact
An EOL version of jQuery 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 jQuery on the remote host to a still supported version.

Vulnerability Detection Method
Checks if an EOL version is present on the target host.
Details: `jQuery End of Life (EOL) Detection (Windows)`
OID:1.3.6.1.4.1.25623.1.0.117148
Version used: `2021-06-11T09:02:34Z`

References
`url: https://github.com/jquery/jquery.com/pull/163`

High (CVSS: 7.5)
NVT: OpenSSL: 1.0.2 < 1.0.2p / 1.1.0 < 1.1.0i Multiple Vulnerabilities (Windows)

Product detection result
`cpe:/a:openssl:openssl:1.0.2j`
`Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)`

Summary
OpenSSL is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version:  1.0.2j
Fixed version:      1.0.2p
Installation
path / port:        80/tcp
```

Impact
Successful exploitation will allow a remote attacker:
- to cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack (CVE-2018-0732).

... continues on next page ...

... continued from previous page ...

- with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key (CVE-2018-0737).

Solution:
Solution type: VendorFix
Upgrade to OpenSSL version 1.1.0i or 1.0.2p or later. See the references for more details.

Affected Software/OS
OpenSSL 1.1.0-1.1.0h and 1.0.2-1.0.2o.

Vulnerability Insight
The flaws exist due to:
- During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client (CVE-2018-0732).
- The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack (CVE-2018-0737).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSL: 1.0.2 < 1.0.2p / 1.1.0 < 1.1.0i Multiple Vulnerabilities (Windows)`
OID:1.3.6.1.4.1.25623.1.0.813153
Version used: `2022-04-13T07:21:45Z`

Product Detection Result
Product: `cpe:/a:openssl:openssl:1.0.2j`
Method: `OpenSSL Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
`cve: CVE-2018-0732`
`cve: CVE-2018-0737`
`url: https://www.openssl.org/news/secadv/20180416.txt`
`url: http://www.securityfocus.com/bid/103766`
`url: http://www.securityfocus.com/bid/104442`
`url: https://www.openssl.org/news/secadv/20180612.txt`
`url: http://seclists.org/oss-sec/2018/q2/50`
`url: https://github.com/openssl/openssl/commit/ea7abeeabf92b7aca160bdd0208636d4d`
`↪a69f4f4`
`url: https://github.com/openssl/openssl/commit/3984ef0b72831da8b3ece4745cac4f857`
`↪5b19098`
`url: https://github.com/openssl/openssl/commit/6939eab03a6e23d2bd2c3f5e34fe1d48e`
`↪542e787`
`url: https://github.com/openssl/openssl/commit/349a41da1ad88ad87825414752a8ff5fd`
`↪d6a6c3f`
`cert-bund: CB-K22/0045`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K20/0324
cert-bund: CB-K19/0313
cert-bund: CB-K19/0054
cert-bund: CB-K19/0052
cert-bund: CB-K19/0049
cert-bund: CB-K19/0046
cert-bund: CB-K19/0045
cert-bund: CB-K19/0044
cert-bund: CB-K18/1075
cert-bund: CB-K18/1011
cert-bund: CB-K18/1006
cert-bund: CB-K18/0595
dfn-cert: DFN-CERT-2019-2456
dfn-cert: DFN-CERT-2019-2157
dfn-cert: DFN-CERT-2019-2030
dfn-cert: DFN-CERT-2019-1996
dfn-cert: DFN-CERT-2019-1897
dfn-cert: DFN-CERT-2019-1722
dfn-cert: DFN-CERT-2019-1285
dfn-cert: DFN-CERT-2019-1240
dfn-cert: DFN-CERT-2019-1238
dfn-cert: DFN-CERT-2019-1108
dfn-cert: DFN-CERT-2019-1101
dfn-cert: DFN-CERT-2019-0777
dfn-cert: DFN-CERT-2019-0441
dfn-cert: DFN-CERT-2019-0294
dfn-cert: DFN-CERT-2019-0204
dfn-cert: DFN-CERT-2019-0200
dfn-cert: DFN-CERT-2019-0119
dfn-cert: DFN-CERT-2019-0111
dfn-cert: DFN-CERT-2019-0110
dfn-cert: DFN-CERT-2019-0103
dfn-cert: DFN-CERT-2019-0058
dfn-cert: DFN-CERT-2018-2539
dfn-cert: DFN-CERT-2018-2456
dfn-cert: DFN-CERT-2018-2396
dfn-cert: DFN-CERT-2018-2210
dfn-cert: DFN-CERT-2018-2106
dfn-cert: DFN-CERT-2018-2103
dfn-cert: DFN-CERT-2018-1980
dfn-cert: DFN-CERT-2018-1832
dfn-cert: DFN-CERT-2018-1825
dfn-cert: DFN-CERT-2018-1709
dfn-cert: DFN-CERT-2018-1664
dfn-cert: DFN-CERT-2018-1485
dfn-cert: DFN-CERT-2018-1308
dfn-cert: DFN-CERT-2018-1224

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2018-1138
dfn-cert: DFN-CERT-2018-0720

High (CVSS: 9.8)
NVT: OpenSSL: c_rehash script allows command injection (CVE-2022-1292) - Windows

Product detection result
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary
OpenSSL is prone to a command injection vulnerability.

Vulnerability Detection Result
Installed version: 1.0.2j
Fixed version: 1.0.2ze
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 1.0.2ze, 1.1.1o or later.

Affected Software/OS
OpenSSL version 1.0.2 and 1.1.1.

Vulnerability Insight
The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSL: c_rehash script allows command injection (CVE-2022-1292) - Windows
OID:1.3.6.1.4.1.25623.1.0.148046
Version used: 2022-05-13T03:03:55Z

Product Detection Result
Product: cpe:/a:openssl:openssl:1.0.2j
Method: OpenSSL Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.145462)

... continues on next page ...

... continued from previous page ...

References
cve: CVE-2022-1292
url: https://www.openssl.org/news/secadv/20220503.txt
cert-bund: CB-K22/0536
dfn-cert: DFN-CERT-2022-1103
dfn-cert: DFN-CERT-2022-0986

High (CVSS: 10.0)
NVT: OpenSSL End of Life (EOL) Detection (Windows)

Product detection result
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary
The OpenSSL version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result
The "OpenSSL" version on the remote host has reached the end of life.
CPE: cpe:/a:openssl:openssl:1.0.2j
Installed version: 1.0.2j
Location/URL: 80/tcp
EOL version: 1.0.2
EOL date: 2019-12-31

Impact
An EOL version of OpenSSL 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 OpenSSL version on the remote host to a still supported version.

Vulnerability Detection Method
Checks if an EOL version is present on the target host.
Details: OpenSSL End of Life (EOL) Detection (Windows)
OID:1.3.6.1.4.1.25623.1.0.113027
Version used: 2021-03-10T05:21:16Z

Product Detection Result
Product: cpe:/a:openssl:openssl:1.0.2j
Method: OpenSSL Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.145462)

... continues on next page ...

... continued from previous page ...

References
url: https://www.openssl.org/policies/releasestrat.html

High (CVSS: 7.5)
NVT: OpenSSL: Infinite loop in BN_mod_sqrt() reachable when parsing certificates (CVE-2022-0778) - Windows

Product detection result
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary
OpenSSL is prone to an infinite loop vulnerability.

Vulnerability Detection Result
Installed version: 1.0.2j
Fixed version: 1.0.2zd
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 1.0.2zd, 1.1.1n, 3.0.2 or later.

Affected Software/OS
OpenSSL version 1.0.2, 1.1.1 and 3.0.0.

Vulnerability Insight
The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli.
Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form.
It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters.
Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters.
Thus vulnerable situations include:
- TLS clients consuming server certificates
- TLS servers consuming client certificates
- Hosting providers taking certificates or private keys from customers
- Certificate authorities parsing certification requests from subscribers

... continues on next page ...

... continued from previous page ...

- Anything else which parses ASN.1 elliptic curve parameters
Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue.
In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSL: Infinite loop in BN_mod_sqrt() reachable when parsing certificates (CV.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.147808
Version used: `2022-03-23T03:03:46Z`

Product Detection Result
Product: `cpe:/a:openssl:openssl:1.0.2j`
Method: `OpenSSL Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
`cve: CVE-2022-0778`
`url: https://www.openssl.org/news/secadv/20220315.txt`
`cert-bund: CB-K22/0619`
`cert-bund: CB-K22/0470`
`cert-bund: CB-K22/0468`
`cert-bund: CB-K22/0321`
`dfn-cert: DFN-CERT-2022-1116`
`dfn-cert: DFN-CERT-2022-1115`
`dfn-cert: DFN-CERT-2022-1114`
`dfn-cert: DFN-CERT-2022-1081`
`dfn-cert: DFN-CERT-2022-0955`
`dfn-cert: DFN-CERT-2022-0902`
`dfn-cert: DFN-CERT-2022-0899`
`dfn-cert: DFN-CERT-2022-0898`
`dfn-cert: DFN-CERT-2022-0873`
`dfn-cert: DFN-CERT-2022-0866`
`dfn-cert: DFN-CERT-2022-0865`
`dfn-cert: DFN-CERT-2022-0779`
`dfn-cert: DFN-CERT-2022-0759`
`dfn-cert: DFN-CERT-2022-0627`
`dfn-cert: DFN-CERT-2022-0625`
`dfn-cert: DFN-CERT-2022-0610`
`dfn-cert: DFN-CERT-2022-0603`

High (CVSS: 7.5)
NVT: OpenSSL: Integer overflow in CipherUpdate (CVE-2021-23840) - Windows

Product detection result
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary
OpenSSL is prone to an integer overflow vulnerability.

Vulnerability Detection Result
Installed version: 1.0.2j
Fixed version: 1.0.2y / 1.1.1j
Installation
path / port: 80/tcp

Impact
This vulnerability could cause applications to behave incorrectly or crash.

Solution:
Solution type: VendorFix
Update to version 1.0.2y, 1.1.1j or later. See the references for more details.

Affected Software/OS
OpenSSL versions 1.0.2x and prior and 1.1.1i and prior.

Vulnerability Insight
Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissible length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSL: Integer overflow in CipherUpdate (CVE-2021-23840) - Windows
OID:1.3.6.1.4.1.25623.1.0.145408
Version used: 2021-08-30T10:29:27Z

Product Detection Result
Product: cpe:/a:openssl:openssl:1.0.2j
Method: OpenSSL Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
cve: CVE-2021-23840

. . . continues on next page . . .

... continued from previous page ...

```
url: https://www.openssl.org/news/secadv/20210216.txt
cert-bund: CB-K22/0061
cert-bund: CB-K21/0389
cert-bund: CB-K21/0185
dfn-cert: DFN-CERT-2022-1215
dfn-cert: DFN-CERT-2022-0121
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2394
dfn-cert: DFN-CERT-2021-2223
dfn-cert: DFN-CERT-2021-2216
dfn-cert: DFN-CERT-2021-2214
dfn-cert: DFN-CERT-2021-1996
dfn-cert: DFN-CERT-2021-1803
dfn-cert: DFN-CERT-2021-1670
dfn-cert: DFN-CERT-2021-1547
dfn-cert: DFN-CERT-2021-1418
dfn-cert: DFN-CERT-2021-1061
dfn-cert: DFN-CERT-2021-0862
dfn-cert: DFN-CERT-2021-0829
dfn-cert: DFN-CERT-2021-0818
dfn-cert: DFN-CERT-2021-0806
dfn-cert: DFN-CERT-2021-0740
dfn-cert: DFN-CERT-2021-0409
dfn-cert: DFN-CERT-2021-0379
dfn-cert: DFN-CERT-2021-0363
```

High (CVSS: 7.4)
NVT: OpenSSL: Read Buffer Overruns Processing ASN.1 Strings (20210824) - Windows

Product detection result

```
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
```

Summary

OpenSSL is prone to a buffer overflow vulnerability.

Vulnerability Detection Result

```
Installed version: 1.0.2j
Fixed version:     1.0.2za / 1.1.1l
Installation
path / port:       80/tcp
```

Impact

... continues on next page ...

... continued from previous page ...

If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext).

Solution:
Solution type: VendorFix
Update to version 1.0.2za, 1.1.1l or later.

Affected Software/OS
OpenSSL 1.1.1 through 1.1.1k and 1.0.2 through 1.0.2y.
Note: OpenSSL 1.0.2 is out of support and no longer receiving public updates. Extended support is available for premium support customers.

Vulnerability Insight
ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are represented as a buffer for the string data which is terminated with a NUL (0) byte.
Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own 'd2i' functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure.
However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the 'data' and 'length' fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function.
Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the 'data' field, then a read buffer overrun can occur.
The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures).
It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSL: Read Buffer Overruns Processing ASN.1 Strings (20210824) - Windows`
OID:1.3.6.1.4.1.25623.1.0.112982
Version used: `2021-09-06T09:01:34Z`

Product Detection Result
Product: `cpe:/a:openssl:openssl:1.0.2j`

... continues on next page ...

... continued from previous page ...

Method: OpenSSL Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.145462)

References

cve: CVE-2021-3712
url: https://www.openssl.org/news/secadv/20210824.txt
cert-bund: CB-K22/0224
cert-bund: CB-K22/0077
cert-bund: CB-K22/0072
cert-bund: CB-K22/0062
cert-bund: CB-K22/0045
cert-bund: CB-K22/0011
cert-bund: CB-K21/1268
cert-bund: CB-K21/1087
cert-bund: CB-K21/0907
dfn-cert: DFN-CERT-2022-1215
dfn-cert: DFN-CERT-2022-0437
dfn-cert: DFN-CERT-2022-0122
dfn-cert: DFN-CERT-2022-0120
dfn-cert: DFN-CERT-2022-0118
dfn-cert: DFN-CERT-2022-0112
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2022-0031
dfn-cert: DFN-CERT-2021-2481
dfn-cert: DFN-CERT-2021-2434
dfn-cert: DFN-CERT-2021-2403
dfn-cert: DFN-CERT-2021-2394
dfn-cert: DFN-CERT-2021-2223
dfn-cert: DFN-CERT-2021-2188
dfn-cert: DFN-CERT-2021-1996
dfn-cert: DFN-CERT-2021-1871
dfn-cert: DFN-CERT-2021-1803
dfn-cert: DFN-CERT-2021-1799

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) - Windows

Product detection result

cpe:/a:php:php:5.6.30
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.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Installed version: 5.6.30
Fixed version:     7.3.32 (not released yet)
Installation
path / port:       80/tcp
```

Solution:
Solution type: VendorFix
Update to version 7.3.32 (not released yet), 7.4.25, 8.0.12 or later.

Affected Software/OS
PHP versions 5.3.7 through 7.3.31, 7.4.x through 7.4.24 and 8.0.x through 8.0.11.
Note: While the referenced CVE is only listing PHP 7.3.x, 7.4.x and 8.0.x as affected the security research team is stating in the linked blog post that all versions down to 5.3.7 are affected.

Vulnerability Insight
Fixed bug #81026 (PHP-FPM oob R/W in root process leading to privilege escalation).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 5.3.7 - 7.3.31, 7.4.x < 7.4.25, 8.0.x < 8.0.12 Security Update (Oct 2021) -. ↪..`
OID:1.3.6.1.4.1.25623.1.0.117753
Version used: `2021-11-05T03:03:34Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
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: CB-K21/1106
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
```

High (CVSS: 9.8)
NVT: PHP < 7.0.12 RCE / DoS Vulnerability - Windows

Product detection result
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a remote code execution (RCE) or denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 7.0.12
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 7.0.12 or later.

Affected Software/OS
PHP versions prior to 7.0.12.

Vulnerability Insight
The SplObjectStorage unserialize implementation in ext/spl/spl_observer.c does not verify that a key is an object, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access) via crafted serialized data.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.0.12 RCE / DoS Vulnerability - Windows
OID:1.3.6.1.4.1.25623.1.0.117801
Version used: 2021-11-29T14:44:44Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2016-7480
url: https://www.php.net/ChangeLog-7.php#7.0.12
url: https://bugs.php.net/bug.php?id=73257
url: http://blog.checkpoint.com/2016/12/27/check-point-discovers-three-zero-day-
↪vulnerabilities-web-programming-language-php-7

. . . continues on next page . . .

... continued from previous page ...

cert-bund: CB-K17/0318
dfn-cert: DFN-CERT-2017-0325

High (CVSS: 9.8)
NVT: PHP <= 7.1.5 Multiple DoS Vulnerabilities

Product detection result
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple denial of service (DoS) vulnerabilities.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: None
Installation
path / port: 80/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
PHP versions through 7.1.5.

Vulnerability Insight
The following flaws exist:
- CVE-2017-8923: The zend_string_extend function in Zend/zend_string.h does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.
- CVE-2017-9119: The i_zval_ptr_dtor function in Zend/zend_variables.h allows attackers to cause a denial of service (memory consumption and application crash) or possibly have unspecified other impact by triggering crafted operations on array data structures.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP <= 7.1.5 Multiple DoS Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.117799
Version used: 2021-11-26T16:17:05Z

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:5.6.30
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2017-8923
cve: CVE-2017-9119
url: https://bugs.php.net/bug.php?id=73122
url: https://bugs.php.net/bug.php?id=74310
url: https://bugs.php.net/bug.php?id=74577
url: https://bugs.php.net/bug.php?id=74593
url: http://www.securityfocus.com/bid/98518
url: http://www.securityfocus.com/bid/98596
dfn-cert: DFN-CERT-2022-0485
dfn-cert: DFN-CERT-2022-0455
dfn-cert: DFN-CERT-2022-0431
dfn-cert: DFN-CERT-2022-0410

High (CVSS: 9.1)
NVT: PHP < 7.2.27, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities - Jan20 (Windows)

Product detection result
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 7.2.27
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 7.2.27, 7.3.14, 7.4.2 or later.

Affected Software/OS
PHP versions before 7.2.27, 7.3.x and 7.4.x.

Vulnerability Insight
PHP is prone to multiple vulnerabilities:

... continues on next page ...

... continued from previous page ...

- OOB read in php_strip_tags_ex (CVE-2020-7059)
- Global buffer-overflow in 'mbfl_filt_conv_big5_wchar' (CVE-2020-7060)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP < 7.2.27, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities - Jan20 (W.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.143393
Version used: `2021-07-08T11:00:45Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2020-7059`
`cve: CVE-2020-7060`
`url: https://www.php.net/ChangeLog-7.php#7.2.27`
`url: https://www.php.net/ChangeLog-7.php#7.3.14`
`url: https://www.php.net/ChangeLog-7.php#7.4.2`
`cert-bund: CB-K20/1199`
`cert-bund: CB-K20/0067`
`dfn-cert: DFN-CERT-2020-2627`
`dfn-cert: DFN-CERT-2020-1964`
`dfn-cert: DFN-CERT-2020-0485`
`dfn-cert: DFN-CERT-2020-0422`
`dfn-cert: DFN-CERT-2020-0415`
`dfn-cert: DFN-CERT-2020-0382`
`dfn-cert: DFN-CERT-2020-0342`
`dfn-cert: DFN-CERT-2020-0339`
`dfn-cert: DFN-CERT-2020-0337`
`dfn-cert: DFN-CERT-2020-0139`

High (CVSS: 7.5)
NVT: PHP < 7.2.30, 7.3 < 7.3.17, 7.4 < 7.4.5 DoS Vulnerability - Apr20 (Windows)

Product detection result
`cpe:/a:php:php:5.6.30`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to a denial-of-service vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Installed version: 5.6.30
Fixed version:     7.2.30
Installation
path / port:       80/tcp
```

Solution:
Solution type: VendorFix
Update to version 7.2.30, 7.3.17, 7.4.5 or later.

Affected Software/OS
PHP versions prior 7.2.30, 7.3 prior 7.3.17 and 7.4 prior to 7.4.5.

Vulnerability Insight
If 'CHARSET_EBCDIC' is defined (usually, on systems with EBCDIC encoding support), an out-of-bounds read can occur using a malformed url-encoded string.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP < 7.2.30, 7.3 < 7.3.17, 7.4 < 7.4.5 DoS Vulnerability - Apr20 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.143723
Version used: `2021-07-08T11:00:45Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
cve: CVE-2020-7067
url: https://www.php.net/ChangeLog-7.php#7.2.30
url: https://www.php.net/ChangeLog-7.php#7.3.17
url: https://www.php.net/ChangeLog-7.php#7.4.5
cert-bund: CB-K20/1199
cert-bund: CB-K20/0336
dfn-cert: DFN-CERT-2020-1438
dfn-cert: DFN-CERT-2020-0851
dfn-cert: DFN-CERT-2020-0751
```

High (CVSS: 7.5)
NVT: PHP < 7.2.32, 7.3 < 7.3.20, 7.4 < 7.4.8 libcurl Vulnerability - May20 (Windows)

Product detection result

```
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

... continues on next page ...

... continued from previous page ...

Summary
PHP is prone to an information disclosure vulnerability in libcurl.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 7.2.32
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 7.2.32, 7.3.20, 7.4.8 or later.

Affected Software/OS
PHP versions prior 7.2.32, 7.3 prior 7.3.20 and 7.4 prior to 7.4.8.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.2.32, 7.3 < 7.3.20, 7.4 < 7.4.8 libcurl Vulnerability - May20 (Windows)
OID:1.3.6.1.4.1.25623.1.0.144246
Version used: 2021-07-08T11:00:45Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2020-8169
url: https://www.php.net/ChangeLog-7.php#7.2.32
url: https://www.php.net/ChangeLog-7.php#7.3.20
url: https://www.php.net/ChangeLog-7.php#7.4.8
cert-bund: CB-K20/0684
cert-bund: CB-K20/0619
dfn-cert: DFN-CERT-2021-1329
dfn-cert: DFN-CERT-2021-0807
dfn-cert: DFN-CERT-2021-0663
dfn-cert: DFN-CERT-2020-1347

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) - Windows

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:php:php:5.6.30
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.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 7.3.27
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 7.3.27, 7.4.15, 8.0.2 or later.

Affected Software/OS
PHP versions prior to 7.3.27, 7.4.x prior to 7.4.15 and 8.0.x prior to 8.0.2.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 NULL Deference Vulnerability (Feb 2.
↪..
OID:1.3.6.1.4.1.25623.1.0.145324
Version used: 2021-11-29T15:00:35Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
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: CB-K21/0124
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

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-0380
dfn-cert: DFN-CERT-2021-0246

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) - Windows

Product detection result
cpe:/a:php:php:5.6.30
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.

Vulnerability Detection Result
Installed version: 5.6.30
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) - Windows
OID:1.3.6.1.4.1.25623.1.0.147658
Version used: 2022-03-09T03:03:43Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
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

... continues on next page ...

... continued from previous page ...

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: CB-K22/0201
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0407
dfn-cert: DFN-CERT-2022-0365

High (CVSS: 7.5)
NVT: PHP 'CVE-2017-7189' Improper Input Validation Vulnerability (Windows)

Product detection result
cpe:/a:php:php:5.6.30
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.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: None
Installation
path / port: 80/tcp

Solution:
Solution type: WillNotFix
No solution was made available by the vendor. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
Note: PHP versions 7.0.18 and 7.1.4 introduced a fix which was reverted again in version 7.0.19 / 7.1.5 respectively and the fix wasn't introduced again as of today (08-2020).

Affected Software/OS
All PHP versions since 4.3.0 up to the latest 7.x versions.
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

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: PHP 'CVE-2017-7189' Improper Input Validation Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.108875
Version used: 2021-07-08T11:00:45Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
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 'CVE-2018-19935' - 'imap_mail' Denial of Service Vulnerability (Windows)

Product detection result
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

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

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 5.6.39
Installation
path / port: 80/tcp

Impact
Successful exploitation will allow attackers to cause a denial of service of the affected application.

Solution:
Solution type: VendorFix
Update to version 5.6.39, 7.0.33, 7.1.26, 7.2.14, 7.3.0 or later.

Affected Software/OS
PHP versions 5.x before 5.6.39, 7.0.x before 7.0.33, 7.1.x before 7.1.26 and 7.2.x before 7.2.14.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw exists due to a NULL pointer dereference and application crash via an empty string in the message argument to the imap_mail function of ext/imap/php_imap.c.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'CVE-2018-19935' - 'imap_mail' Denial of Service Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.108506
Version used: `2022-04-13T07:21:45Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2018-19935`
`url: https://bugs.php.net/bug.php?id=77020`
`url: http://www.securityfocus.com/bid/106143`
`cert-bund: CB-K18/1154`
`dfn-cert: DFN-CERT-2019-1181`
`dfn-cert: DFN-CERT-2019-0313`
`dfn-cert: DFN-CERT-2019-0044`
`dfn-cert: DFN-CERT-2018-2476`

High (CVSS: 9.8)
NVT: PHP 'CVE-2019-11043' FPM Remote Code Execution Vulnerability (Version Check)

Product detection result
`cpe:/a:php:php:5.6.30`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to a remote code execution vulnerability in certain nginx + php-fpm configurations.

Vulnerability Detection Result
```
Installed version: 5.6.30
Fixed version:     7.1.33
Installation
path / port:       80/tcp
```

Impact
Successful exploitation would allow an unauthenticated remote attacker to execute arbitrary code on the target machine.

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Update to version 7.1.33, 7.2.24, 7.3.11 or later. As an alternative a workaround to update the nginx configuration to mitigate this vulnerability is described at the PHP.net bugtracker linked in the references.

Affected Software/OS
PHP versions before 7.1.33, 7.2.x before 7.2.24 and 7.3.x before 7.3.11.

Vulnerability Insight
The file sapi/fpm/fpm/fpm_main.c contains pointer arithmetic that assumes that env_path_info has a prefix equal to the path to the php script. However, the code does not check this assumption is satisfied. The absence of the check can lead to an invalid pointer in the 'path_info' variable.
Such conditions can be achieved in a pretty standard Nginx configuration. The regexp in 'fastcgi_split_path_info' directive can be broken using the newline character (in encoded form, %0a). Broken regexp leads to empty PATH_INFO, which triggers the bug.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'CVE-2019-11043' FPM Remote Code Execution Vulnerability (Version Check)`
OID:1.3.6.1.4.1.25623.1.0.108692
Version used: `2021-08-30T14:01:20Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2019-11043`
`url: https://bugs.php.net/bug.php?id=78599`
`url: https://www.php.net/ChangeLog-7.php#7.3.11`
`url: https://www.php.net/ChangeLog-7.php#7.2.24`
`url: https://www.php.net/ChangeLog-7.php#7.1.33`
`url: https://github.com/neex/phuip-fpizdam`
`cert-bund: CB-K20/0081`
`cert-bund: CB-K19/0943`
`dfn-cert: DFN-CERT-2020-0415`
`dfn-cert: DFN-CERT-2020-0193`
`dfn-cert: DFN-CERT-2019-2283`
`dfn-cert: DFN-CERT-2019-2206`

High (CVSS: 9.8)
NVT: PHP 'CVE-2019-13224' Use-After-Free Vulnerability (Windows)

Product detection result
`cpe:/a:php:php:5.6.30`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to a use-after-free vulnerability in a used third-pary library.

Vulnerability Detection Result
`Installed version: 5.6.30`
`Fixed version: 7.1.32`
`Installation path / port: 80/tcp`

Impact
This flaw allows attackers to potentially cause information disclosure, denial of service, or possibly code execution by providing a crafted regular expression.

Solution:
Solution type: VendorFix
Update to version 7.1.32, 7.3.9 or later.

Affected Software/OS
PHP version before 7.1.32 and 7.3.x before 7.3.9.

Vulnerability Insight
The flaw exists due to a use-after-free in onig_new_deluxe() in regext.c of the third-party library Oniguruma 6.9.2 which is used by PHP.
The attacker provides a pair of a regex pattern and a string, with a multi-byte encoding that gets handled by onig_new_deluxe().

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'CVE-2019-13224' Use-After-Free Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.108634
Version used: `2021-08-30T14:01:20Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
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-2019-13224
url: http://bugs.php.net/78380
url: https://www.php.net/ChangeLog-7.php#7.3.9
url: https://www.php.net/ChangeLog-7.php#7.1.32
cert-bund: CB-K20/1030
dfn-cert: DFN-CERT-2020-2412
dfn-cert: DFN-CERT-2020-2105
dfn-cert: DFN-CERT-2020-1964
dfn-cert: DFN-CERT-2019-1804
dfn-cert: DFN-CERT-2019-1471
dfn-cert: DFN-CERT-2019-1424
```

High (CVSS: 7.5)
NVT: PHP Denial of Service Vulnerability Jul17 (Windows)

Product detection result
`cpe:/a:php:php:5.6.30`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

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

Vulnerability Detection Result
```
Installed version: 5.6.30
Fixed version:     5.6.31
```

Impact
Successfully exploiting this issue allow an attacker to cause a CPU consumption denial of service attack.

Solution:
Solution type: VendorFix
Update to PHP version 5.6.31, 7.0.17, 7.1.3 or later.

Affected Software/OS
PHP versions before 5.6.31, 7.x before 7.0.17, and 7.1.x before 7.1.3

Vulnerability Insight
The flaw exists due to improper handling of long form variables in main/php_variables.c script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Denial of Service Vulnerability Jul17 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.811486

... continues on next page ...

... continued from previous page ...

Version used: 2021-09-10T08:01:37Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2017-11142
url: http://www.php.net/ChangeLog-5.php
url: http://www.php.net/ChangeLog-7.php
cert-bund: CB-K18/0048
cert-bund: CB-K17/1461
cert-bund: CB-K17/1132
dfn-cert: DFN-CERT-2018-0055
dfn-cert: DFN-CERT-2017-1529
dfn-cert: DFN-CERT-2017-1161

High (CVSS: 10.0)
NVT: PHP End Of Life Detection (Windows)

Product detection result
cpe:/a:php:php:5.6.30
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 and should not be used anymore.

Vulnerability Detection Result
The "PHP" version on the remote host has reached the end of life.
CPE: cpe:/a:php:php:5.6.30
Installed version: 5.6.30
EOL version: 5.6
EOL date: 2018-12-31

Impact
An end of life 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

... continues on next page ...

... continued from previous page ...

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 a vulnerable version is present on the target host.
Details: `PHP End Of Life Detection (Windows)`
OID:1.3.6.1.4.1.25623.1.0.105888
Version used: `2021-04-13T14:13:08Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
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: 7.5)
NVT: phpinfo() output Reporting

Summary
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 Result
```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information:
http://13.58.47.204/dashboard/phpinfo.php
```

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.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details: `phpinfo() output Reporting`
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: `2020-08-24T15:18:35Z`

High (CVSS: 7.5)
NVT: PHP Multiple Heap Buffer Overflow and Information Disclosure Vulnerabilities (Windows)

Product detection result
`cpe:/a:php:php:5.6.30`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to multiple heap buffer overflow and information disclosure vulnerabilities.

Vulnerability Detection Result
```
Installed version: 5.6.30
Fixed version:     5.6.37
Installation
path / port:       80/tcp
```

Impact
Successful exploitation will allow attackers to cause heap overflow, denial of service and disclose sensitive information.

Solution:
Solution type: VendorFix
Update to PHP version 5.6.37, 7.0.31, 7.1.20 or 7.2.8 or later. Please see the references for more information.

Affected Software/OS
PHP versions before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8.

Vulnerability Insight
Multiple flaws exist due to:
- exif_process_IFD_in_MAKERNOTE function in exif.c file suffers from improper validation against crafted JPEG files.
- exif_thumbnail_extract function in exif.c file suffers from improper validation of length of 'ImageInfo->Thumbnail.offset + ImageInfo->Thumbnail.size'
- linkinfo function on windows doesn't implement openbasedir check.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: PHP Multiple Heap Buffer Overflow and Information Disclosure Vulnerabilities (W.
↪..
OID:1.3.6.1.4.1.25623.1.0.813597
Version used: 2021-08-10T15:24:26Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2018-14851
cve: CVE-2018-14883
cve: CVE-2018-15132
url: https://access.redhat.com/security/cve/cve-2018-14851
url: https://bugs.php.net/bug.php?id=76557
url: https://bugs.php.net/bug.php?id=76423
url: https://bugs.php.net/bug.php?id=76459
cert-bund: CB-K18/0838
dfn-cert: DFN-CERT-2019-1737
dfn-cert: DFN-CERT-2018-2116
dfn-cert: DFN-CERT-2018-1882
dfn-cert: DFN-CERT-2018-1835
dfn-cert: DFN-CERT-2018-1834
dfn-cert: DFN-CERT-2018-1777
dfn-cert: DFN-CERT-2018-1655

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - Dec18 (Windows)

Product detection result
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple security vulnerabilities.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 5.6.39
Installation
path / port: 80/tcp

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attackers to execute remote code on the affected application/system and/or cause a cause a denial of service.

Solution:
Solution type: VendorFix
Update to version 5.6.39, 7.0.33, 7.1.25, 7.2.13, 7.3.0 or later.

Affected Software/OS
PHP versions 5.x before 5.6.39, 7.0.x before 7.0.33, 7.1.x before 7.1.25 and 7.2.x before 7.2.13.

Vulnerability Insight
The flaws exist due to:
- the imap_open functions which allows to run arbitrary shell commands via mailbox parameter.
- a Heap Buffer Overflow (READ: 4) in phar_parse_pharfile.
- ext/standard/var_unserializer.c allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.
- because com and com_safearray_proxy return NULL in com_properties_get in ext/com_dotnet/com_handlers.c, as demonstrated by a serialize call on COM('WScript.Shell').

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - Dec18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.108508
Version used: `2022-04-20T03:02:11Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2018-19518`
`cve: CVE-2018-20783`
`cve: CVE-2018-19395`
`cve: CVE-2018-19396`
`url: https://bugs.php.net/bug.php?id=76428`
`url: https://bugs.php.net/bug.php?id=77153`
`url: https://bugs.php.net/bug.php?id=77160`
`url: https://bugs.php.net/bug.php?id=77143`
`url: http://www.securityfocus.com/bid/106018`
`url: https://github.com/Bo0oM/PHP_imap_open_exploit/blob/master/exploit.php`
`url: https://www.exploit-db.com/exploits/45914/`
`url: https://www.openwall.com/lists/oss-security/2018/11/22/3`
`cert-bund: CB-K18/1118`
`dfn-cert: DFN-CERT-2020-0898`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2019-2283
dfn-cert: DFN-CERT-2019-1737
dfn-cert: DFN-CERT-2019-1181
dfn-cert: DFN-CERT-2019-1052
dfn-cert: DFN-CERT-2019-0804
dfn-cert: DFN-CERT-2019-0698
dfn-cert: DFN-CERT-2019-0440
dfn-cert: DFN-CERT-2018-2488
dfn-cert: DFN-CERT-2018-2476

High (CVSS: 9.8)
NVT: PHP Multiple Vulnerabilities (Feb 2019) - Windows

Product detection result
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 5.6.40
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 5.6.40, 7.1.16, 7.2.14, 7.3.1 or later.

Affected Software/OS
PHP versions before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14 and 7.3.x before 7.3.1.

Vulnerability Insight
The following flaws exist:
- Fixed bug #77269 (efree() on uninitialized Heap data in imagescale leads to use-after-free). (CVE-2016-10166)
- Fixed bug #77270 (imagecolormatch Out Of Bounds Write on Heap). (CVE-2019-6977)
- Fixed bug #77370 (Buffer overflow on mb regex functions - fetch_token). (CVE-2019-9023)
- Fixed bug #77371 (heap buffer overflow in mb regex functions - compile_string_node). (CVE-2019-9023)
- Fixed bug #77381 (heap buffer overflow in multibyte match_at). (CVE-2019-9023)
- Fixed bug #77382 (heap buffer overflow due to incorrect length in expand_case_fold_string). (CVE-2019-9023)
- Fixed bug #77385 (buffer overflow in fetch_token). (CVE-2019-9023)

... continues on next page ...

... continued from previous page ...

- Fixed bug #77394 (Buffer overflow in multibyte case folding - unicode). (CVE-2019-9023)
- Fixed bug #77418 (Heap overflow in utf32be_mbc_to_code). (CVE-2019-9023)
- Fixed bug #77247 (heap buffer overflow in phar_detect_phar_fname_ext). (CVE-2019-9021)
- Fixed bug #77242 (heap out of bounds read in xmlrpc_decode()). (CVE-2019-9020)
- Fixed bug #77380 (Global out of bounds read in xmlrpc base64 code). (CVE-2019-9024)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities (Feb 2019) - Windows`
OID:1.3.6.1.4.1.25623.1.0.142049
Version used: `2021-11-26T13:39:39Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2016-10166`
`cve: CVE-2019-9020`
`cve: CVE-2019-9021`
`cve: CVE-2019-9023`
`cve: CVE-2019-9024`
`cve: CVE-2019-6977`
`url: http://www.php.net/ChangeLog-5.php`
`url: http://www.php.net/ChangeLog-7.php`
`url: https://bugs.php.net/bug.php?id=77269`
`url: https://bugs.php.net/bug.php?id=77270`
`url: https://bugs.php.net/bug.php?id=77370`
`url: https://bugs.php.net/bug.php?id=77371`
`url: https://bugs.php.net/bug.php?id=77381`
`url: https://bugs.php.net/bug.php?id=77382`
`url: https://bugs.php.net/bug.php?id=77385`
`url: https://bugs.php.net/bug.php?id=77394`
`url: https://bugs.php.net/bug.php?id=77418`
`url: https://bugs.php.net/bug.php?id=77247`
`url: https://bugs.php.net/bug.php?id=77242`
`url: https://bugs.php.net/bug.php?id=77380`
`cert-bund: CB-K19/0166`
`cert-bund: CB-K17/1252`
`cert-bund: CB-K17/0318`
`cert-bund: CB-K17/0232`
`cert-bund: CB-K17/0182`
`dfn-cert: DFN-CERT-2020-2398`
`dfn-cert: DFN-CERT-2020-1078`
`dfn-cert: DFN-CERT-2020-0898`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2020-0680
dfn-cert: DFN-CERT-2019-2283
dfn-cert: DFN-CERT-2019-1737
dfn-cert: DFN-CERT-2019-1181
dfn-cert: DFN-CERT-2019-0804
dfn-cert: DFN-CERT-2019-0698
dfn-cert: DFN-CERT-2019-0434
dfn-cert: DFN-CERT-2019-0368
dfn-cert: DFN-CERT-2019-0313
dfn-cert: DFN-CERT-2019-0241
dfn-cert: DFN-CERT-2019-0212
dfn-cert: DFN-CERT-2017-1295
dfn-cert: DFN-CERT-2017-0325
dfn-cert: DFN-CERT-2017-0234
dfn-cert: DFN-CERT-2017-0179
```

High (CVSS: 9.8)
NVT: PHP Multiple Vulnerabilities (Jul 2017 - 01) - Windows

Product detection result

```
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.6.30
Fixed version:     5.6.31
Installation
path / port:       80/tcp
```

Impact

Successfully exploiting this issue allow remote attackers to leak information from the interpreter, crash PHP interpreter and also disclose sensitive information.

Solution:

Solution type: VendorFix

Update to version 5.6.31, 7.0.21, 7.1.7 or later.

Affected Software/OS

PHP versions before 5.6.31, 7.x before 7.0.21 and 7.1.x before 7.1.7.

Vulnerability Insight

Multiple flaws are due to:

... continues on next page ...

... continued from previous page ...

- An ext/date/lib/parse_date.c out-of-bounds read affecting the php_parse_date function.
- The openssl extension PEM sealing code did not check the return value of the OpenSSL sealing function.
- lack of bounds checks in the date extension's timelib_meridian parsing code.
- A stack-based buffer overflow in the zend_ini_do_op() function in the 'Zend/zend_ini_parser.c' script.
- The GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd) does not zero colorMap arrays before use.
- Heap buffer overread (READ: 1) finish_nested_data from unserialize
- Add oniguruma upstream fix

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities (Jul 2017 - 01) - Windows`
OID:1.3.6.1.4.1.25623.1.0.811481
Version used: `2022-04-13T11:57:07Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2017-7890`
`cve: CVE-2017-9224`
`cve: CVE-2017-9225`
`cve: CVE-2017-9226`
`cve: CVE-2017-9227`
`cve: CVE-2017-9228`
`cve: CVE-2017-9229`
`cve: CVE-2017-11144`
`cve: CVE-2017-11145`
`cve: CVE-2017-11628`
`cve: CVE-2017-12933`
`url: http://www.php.net/ChangeLog-5.php`
`url: http://www.securityfocus.com/bid/99492`
`url: http://www.securityfocus.com/bid/99550`
`url: http://www.securityfocus.com/bid/99605`
`url: http://www.securityfocus.com/bid/99612`
`url: http://www.securityfocus.com/bid/99489`
`url: http://www.php.net/ChangeLog-7.php`
`cert-bund: CB-K18/0270`
`cert-bund: CB-K18/0048`
`cert-bund: CB-K17/2123`
`cert-bund: CB-K17/1575`
`cert-bund: CB-K17/1573`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K17/1562
cert-bund: CB-K17/1468
cert-bund: CB-K17/1461
cert-bund: CB-K17/1373
cert-bund: CB-K17/1358
cert-bund: CB-K17/1132
cert-bund: CB-K17/1011
cert-bund: CB-K17/0908
dfn-cert: DFN-CERT-2020-1221
dfn-cert: DFN-CERT-2020-0484
dfn-cert: DFN-CERT-2020-0479
dfn-cert: DFN-CERT-2019-1052
dfn-cert: DFN-CERT-2018-2116
dfn-cert: DFN-CERT-2018-0835
dfn-cert: DFN-CERT-2018-0733
dfn-cert: DFN-CERT-2018-0290
dfn-cert: DFN-CERT-2018-0055
dfn-cert: DFN-CERT-2017-2219
dfn-cert: DFN-CERT-2017-1647
dfn-cert: DFN-CERT-2017-1644
dfn-cert: DFN-CERT-2017-1629
dfn-cert: DFN-CERT-2017-1530
dfn-cert: DFN-CERT-2017-1529
dfn-cert: DFN-CERT-2017-1432
dfn-cert: DFN-CERT-2017-1420
dfn-cert: DFN-CERT-2017-1161
dfn-cert: DFN-CERT-2017-1046
dfn-cert: DFN-CERT-2017-0932
```

High (CVSS: 8.8)
NVT: PHP Multiple Vulnerabilities May18 (Windows)

Product detection result

```
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.6.30
Fixed version:     5.6.36
Installation
path / port:       80/tcp
```

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow an attacker to conduct XSS attacks, crash PHP, conduct denial-of-service condition and execute arbitrary code in the context of the affected application.

Solution:
Solution type: VendorFix
Update to version 7.2.5 or 7.0.30 or 5.6.36 or 7.1.17 or later. Please see the references for more information.

Affected Software/OS
PHP versions prior to 5.6.36,
PHP versions 7.2.x prior to 7.2.5,
PHP versions 7.0.x prior to 7.0.30,
PHP versions 7.1.x prior to 7.1.17 on Windows.

Vulnerability Insight
Multiple flaws exist due to
- An out of bounds read error in 'exif_read_data' function while processing crafted JPG data.
- An error in stream filter 'convert.iconv' which leads to infinite loop on invalid sequence.
- An error in the LDAP module of PHP which allows a malicious LDAP server or man-in-the-middle attacker to crash PHP.
- An error in the 'phar_do_404()' function in 'ext/phar/phar_object.c' script which returns parts of the request unfiltered, leading to another XSS vector. This is due to incomplete fix for CVE-2018-5712.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities May18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.813159
Version used: `2021-06-03T02:00:18Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2018-10549`
`cve: CVE-2018-10546`
`cve: CVE-2018-10548`
`cve: CVE-2018-10547`
`url: http://www.php.net/ChangeLog-5.php#5.6.36`
`url: http://www.php.net/ChangeLog-7.php#7.0.30`
`url: http://www.php.net/ChangeLog-7.php#7.1.17`
`url: http://www.php.net/ChangeLog-7.php#7.2.5`
`cert-bund: CB-K18/0633`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-0680
dfn-cert: DFN-CERT-2019-1737
dfn-cert: DFN-CERT-2018-1232
dfn-cert: DFN-CERT-2018-0920
dfn-cert: DFN-CERT-2018-0877

High (CVSS: 9.8)
NVT: PHP Stack Buffer Overflow Vulnerability Mar18 (Windows)

Product detection result
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a stack buffer overflow vulnerability.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 5.6.34
Installation
path / port: 80/tcp

Impact
Successful exploitation will allow an attacker to execute arbitrary code in the context of the affected application. Failed exploit attempts will result in denial-of-service conditions.

Solution:
Solution type: VendorFix
Update to version 7.2.3, 7.0.28, 5.6.34, 7.1.15 or later.

Affected Software/OS
PHP versions 7.2.x prior to 7.2.3,
PHP versions 7.0.x prior to 7.0.28,
PHP versions 5.0.x prior to 5.6.34 and
PHP versions 7.1.x prior to 7.1.15 on Windows.

Vulnerability Insight
The flaw exists because php fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP Stack Buffer Overflow Vulnerability Mar18 (Windows)
OID:1.3.6.1.4.1.25623.1.0.812820

... continues on next page ...

... continued from previous page ...

Version used: 2022-04-13T07:21:45Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2018-7584
url: http://php.net/ChangeLog-7.php
url: http://www.securityfocus.com/bid/103204
url: https://bugs.php.net/bug.php?id=75981
cert-bund: CB-K18/0698
cert-bund: CB-K18/0498
cert-bund: CB-K18/0383
dfn-cert: DFN-CERT-2020-0680
dfn-cert: DFN-CERT-2019-1737
dfn-cert: DFN-CERT-2018-1232
dfn-cert: DFN-CERT-2018-1059
dfn-cert: DFN-CERT-2018-0733
dfn-cert: DFN-CERT-2018-0576
dfn-cert: DFN-CERT-2018-0537
dfn-cert: DFN-CERT-2018-0399

High (CVSS: 7.5)
NVT: PHP 'timelib_meridian' Heap Based Buffer Overflow Vulnerability (Windows)

Product detection result
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a heap buffer overflow vulnerability.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 5.6.32
Installation
path / port: 80/tcp

Impact
Successfully exploiting this issue allow attacker to execute arbitrary code with elevated privileges within the context of a privileged process.

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Update to PHP version 5.6.32, 7.0.25, 7.1.11, or later.

Affected Software/OS
PHP versions before 5.6.32, 7.x before 7.0.25, and 7.1.x before 7.1.11

Vulnerability Insight
The flaw exists due to an error in the date extension's 'timelib_meridian' handling of 'front of' and 'back of' directives.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'timelib_meridian' Heap Based Buffer Overflow Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812072
Version used: `2022-04-13T11:57:07Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2017-16642`
`url: http://php.net/ChangeLog-5.php`
`url: http://www.securityfocus.com/bid/101745`
`url: http://php.net/ChangeLog-7.php`
`url: https://bugs.php.net/bug.php?id=75055`
`cert-bund: CB-K18/0270`
`cert-bund: CB-K18/0048`
`cert-bund: CB-K17/2123`
`dfn-cert: DFN-CERT-2019-1737`
`dfn-cert: DFN-CERT-2018-0835`
`dfn-cert: DFN-CERT-2018-0733`
`dfn-cert: DFN-CERT-2018-0290`
`dfn-cert: DFN-CERT-2018-0055`
`dfn-cert: DFN-CERT-2017-2219`

High (CVSS: 7.5)
NVT: PHP 'WDDX Deserialization' Denial of Service Vulnerability - (Windows)

Product detection result
`cpe:/a:php:php:5.6.30`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Result
`Installed version: 5.6.30`
`Fixed version: 5.6.31`

Impact
Successfully exploiting this issue allow remote attackers inject XML for deserialization to crash the PHP interpreter.

Solution:
Solution type: VendorFix
Update to PHP version 5.6.31 or later.

Affected Software/OS
PHP versions before 5.6.31.

Vulnerability Insight
The flaw exists due to an invalid free error for an empty boolean element in ext/wddx/wddx.c script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'WDDX Deserialization' Denial of Service Vulnerability - (Windows)`
OID:1.3.6.1.4.1.25623.1.0.811485
Version used: `2021-09-16T13:01:47Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2017-11143`
`url: http://www.php.net/ChangeLog-5.php`
`cert-bund: CB-K18/0048`
`cert-bund: CB-K17/1461`
`cert-bund: CB-K17/1358`
`cert-bund: CB-K17/1132`
`dfn-cert: DFN-CERT-2018-0835`
`dfn-cert: DFN-CERT-2018-0733`
`dfn-cert: DFN-CERT-2018-0055`
`dfn-cert: DFN-CERT-2017-1529`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2017-1420
dfn-cert: DFN-CERT-2017-1161

High (CVSS: 8.8)
NVT: XAMPP < 7.2.29, 7.3 < 7.3.16, 7.4 < 7.4.4 Configuration Vulnerability

Summary
XAMPP for Windows is prone to a vulnerability where an unprivileged user can change a .exe configuration in xampp-contol.ini for all users (including admins) to enable arbitrary command execution.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 7.2.29
Installation
path / port: /dashboard

Solution:
Solution type: VendorFix
Update to version 7.2.29, 7.3.16, 7.4.4 or later.

Affected Software/OS
XAMPP for Windows versions prior 7.2.29, 7.3.x prior 7.3.16 and 7.4.x prior 7.4.4.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: XAMPP < 7.2.29, 7.3 < 7.3.16, 7.4 < 7.4.4 Configuration Vulnerability
OID:1.3.6.1.4.1.25623.1.0.143676
Version used: 2021-07-08T11:00:45Z

References
cve: CVE-2020-11107
url: https://www.apachefriends.org/blog/new_xampp_20200401.html

[return to 13.58.47.204]

2.1.2 Medium 80/tcp

Medium (CVSS: 6.1)
NVT: Apache HTTP Server 2.4.0 - 2.4.40 Multiple Vulnerabilities (Windows)

Product detection result
cpe:/a:apache:http_server:2.4.25
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1

... continues on next page ...

... continued from previous page ...

↪.0.117232)

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 2.4.25
Fixed version: 2.4.41
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 2.4.41 or later.

Affected Software/OS
Apache HTTP Server version 2.4.0 to 2.4.40.

Vulnerability Insight
Apache HTTP server is prone to multiple vulnerabilities:
- A limited cross-site scripting issue affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed. (CVE-2019-10092)
- Redirects configured with mod_rewrite that were intended to be self referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL. (CVE-2019-10098)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server 2.4.0 - 2.4.40 Multiple Vulnerabilities (Windows)
OID:1.3.6.1.4.1.25623.1.0.114144
Version used: 2021-09-02T13:01:30Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2019-10092
cve: CVE-2019-10098
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K20/1030

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K20/0708
cert-bund: CB-K20/0043
cert-bund: CB-K19/0909
cert-bund: CB-K19/0728
dfn-cert: DFN-CERT-2021-1333
dfn-cert: DFN-CERT-2021-0540
dfn-cert: DFN-CERT-2020-2422
dfn-cert: DFN-CERT-2020-2133
dfn-cert: DFN-CERT-2020-1124
dfn-cert: DFN-CERT-2020-0716
dfn-cert: DFN-CERT-2020-0090
dfn-cert: DFN-CERT-2019-2592
dfn-cert: DFN-CERT-2019-2169
dfn-cert: DFN-CERT-2019-1961
dfn-cert: DFN-CERT-2019-1810
dfn-cert: DFN-CERT-2019-1797
dfn-cert: DFN-CERT-2019-1751
```

Medium (CVSS: 6.1)
NVT: Apache HTTP Server 2.4.0 < 2.4.42 Multiple Vulnerabilities (Windows)

Product detection result

```
cpe:/a:apache:http_server:2.4.25
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.

Vulnerability Detection Result

```
Installed version: 2.4.25
Fixed version:     2.4.42
Installation
path / port:       80/tcp
```

Solution:

Solution type: VendorFix

Update to version 2.4.42 or later.

Affected Software/OS

Apache HTTP Server version 2.4.0 to 2.4.41.

Vulnerability Insight

Apache HTTP Server is prone to multiple vulnerabilities:
- mod_rewrite CWE-601 open redirect (CVE-2020-1927)

... continues on next page ...

... continued from previous page ...

- mod_proxy_ftp use of uninitialized value (CVE-2020-1934)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server 2.4.0 < 2.4.42 Multiple Vulnerabilities (Windows)
OID:1.3.6.1.4.1.25623.1.0.143672
Version used: 2021-07-22T02:00:50Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2020-1927
cve: CVE-2020-1934
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K20/1030
cert-bund: CB-K20/0708
cert-bund: CB-K20/0691
cert-bund: CB-K20/0280
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2021-1467
dfn-cert: DFN-CERT-2020-2422
dfn-cert: DFN-CERT-2020-2133
dfn-cert: DFN-CERT-2020-1854
dfn-cert: DFN-CERT-2020-1793
dfn-cert: DFN-CERT-2020-1538
dfn-cert: DFN-CERT-2020-1335
dfn-cert: DFN-CERT-2020-1289
dfn-cert: DFN-CERT-2020-1124
dfn-cert: DFN-CERT-2020-0850
dfn-cert: DFN-CERT-2020-0835
dfn-cert: DFN-CERT-2020-0688

Medium (CVSS: 5.3)
NVT: Apache HTTP Server < 2.4.38 HTTP/2 DoS Vulnerability (Windows)

Product detection result
cpe:/a:apache:http_server:2.4.25
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary

... continues on next page ...

... continued from previous page ...

By sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.

Vulnerability Detection Result
Installed version: 2.4.25
Fixed version: 2.4.38
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 2.4.38 or later.

Affected Software/OS
Apache HTTP Server version 2.4.37 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server < 2.4.38 HTTP/2 DoS Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.141965
Version used: 2021-09-02T13:01:30Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2018-17189
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K20/0041
cert-bund: CB-K19/0316
cert-bund: CB-K19/0071
dfn-cert: DFN-CERT-2020-2422
dfn-cert: DFN-CERT-2019-2592
dfn-cert: DFN-CERT-2019-2456
dfn-cert: DFN-CERT-2019-0781
dfn-cert: DFN-CERT-2019-0687
dfn-cert: DFN-CERT-2019-0529
dfn-cert: DFN-CERT-2019-0184

Medium (CVSS: 5.3)
NVT: Apache HTTP Server < 2.4.39 mod_http2 Use-After-Free Vulnerability (Windows)

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:apache:http_server:2.4.25
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

Vulnerability Detection Result
Installed version: 2.4.25
Fixed version: 2.4.39
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 2.4.39 or later.

Affected Software/OS
Apache HTTP Server version 2.4.38 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server < 2.4.39 mod_http2 Use-After-Free Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.142227
Version used: 2021-09-02T13:01:30Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2019-0196
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K19/0623
cert-bund: CB-K19/0267
dfn-cert: DFN-CERT-2020-2422
dfn-cert: DFN-CERT-2020-1335
dfn-cert: DFN-CERT-2019-2456
dfn-cert: DFN-CERT-2019-1054
dfn-cert: DFN-CERT-2019-0687

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2019-0676

Medium (CVSS: 5.3)
NVT: Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Windows)

Product detection result
cpe:/a:apache:http_server:2.4.25
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

Vulnerability Detection Result
Installed version: 2.4.25
Fixed version: 2.4.39
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 2.4.39 or later.

Affected Software/OS
Apache HTTP Server version 2.4.38 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.142229
Version used: 2021-09-02T13:01:30Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2019-0220
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K20/0708
cert-bund: CB-K19/0623

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K19/0267
dfn-cert: DFN-CERT-2020-0184
dfn-cert: DFN-CERT-2019-2592
dfn-cert: DFN-CERT-2019-1519
dfn-cert: DFN-CERT-2019-0815
dfn-cert: DFN-CERT-2019-0690
dfn-cert: DFN-CERT-2019-0687
dfn-cert: DFN-CERT-2019-0680
dfn-cert: DFN-CERT-2019-0676
```

Medium (CVSS: 5.3)
NVT: Apache HTTP Server 2.4.6 - 2.4.46 Tunneling Misconfiguration Vulnerability - Windows

Product detection result
`cpe:/a:apache:http_server:2.4.25`
`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 tunneling misconfiguration vulnerability.

Vulnerability Detection Result

```
Installed version: 2.4.25
Fixed version:     2.4.48
Installation
path / port:       80/tcp
```

Solution:
Solution type: VendorFix
Update to version 2.4.48 or later.

Affected Software/OS
Apache HTTP Server versions 2.4.6 to 2.4.46 on Windows.

Vulnerability Insight
mod_proxy_wstunnel configured on an URL that is not necessarily upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server 2.4.6 - 2.4.46 Tunneling Misconfiguration Vulnerability - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.112899

... continues on next page ...

... continued from previous page ...

Version used: 2021-08-24T09:01:06Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.25
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2019-17567
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K21/0646
dfn-cert: DFN-CERT-2021-2394
dfn-cert: DFN-CERT-2021-1273

Medium (CVSS: 5.9)
NVT: Apache HTTP Server Denial of Service Vulnerability Apr18 (Windows)

Product detection result
cpe:/a:apache:http_server:2.4.25
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 vulnerability.

Vulnerability Detection Result
Installed version: 2.4.25
Fixed version: 2.4.30
Installation
path / port: 80/tcp

Impact
Successful exploitation will allow an attacker to destroy an HTTP/2 stream, resulting in a denial of service condition.

Solution:
Solution type: VendorFix
Update to version 2.4.30 or later. Please see the references for more information.

Affected Software/OS
Apache HTTP Server versions 2.4.17, 2.4.18, 2.4.20, 2.4.23 and from 2.4.25 to 2.4.29.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The flaw exists as the Apache HTTP Server writes a NULL pointer potentially to an already freed memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server Denial of Service Vulnerability Apr18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812850
Version used: `2022-04-13T07:21:45Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.25`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
`cve: CVE-2018-1302`
`url: http://www.openwall.com/lists/oss-security/2018/03/24/8`
`url: http://www.securityfocus.com/bid/103528`
`url: http://www.openwall.com/lists/oss-security/2018/03/24/2`
`cert-bund: CB-K18/0535`
`dfn-cert: DFN-CERT-2019-0359`
`dfn-cert: DFN-CERT-2019-0351`
`dfn-cert: DFN-CERT-2018-2011`
`dfn-cert: DFN-CERT-2018-1386`
`dfn-cert: DFN-CERT-2018-0985`
`dfn-cert: DFN-CERT-2018-0570`

Medium (CVSS: 5.9)
NVT: Apache HTTP Server HTTP/2 'SETTINGS' Data Processing DoS Vulnerability (Windows)

Product detection result
`cpe:/a:apache:http_server:2.4.25`
`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 vulnerability.

Vulnerability Detection Result
`Installed version: 2.4.25`
`Fixed version: 2.4.35`
`Installation`
`path / port: 80/tcp`

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow remote attackers to cause a denial of service (DoS) condition on a targeted system.

Solution:
Solution type: VendorFix
Update to Apache HTTP Server 2.4.35 or later. Please see the references for more information.

Affected Software/OS
Apache HTTP Server versions 2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18.

Vulnerability Insight
The flaw is due to an improper processing of specially crafted and continuous SETTINGS data for an ongoing HTTP/2 connection to cause the target service to fail to timeout.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server HTTP/2 'SETTINGS' Data Processing DoS Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.814057
Version used: `2021-06-14T11:00:34Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.25`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
`cve: CVE-2018-11763`
`url: https://securitytracker.com/id/1041713`
`url: https://httpd.apache.org/security/vulnerabilities_24.html`
`cert-bund: CB-K19/0316`
`cert-bund: CB-K19/0050`
`cert-bund: CB-K18/0949`
`dfn-cert: DFN-CERT-2019-1562`
`dfn-cert: DFN-CERT-2019-0359`
`dfn-cert: DFN-CERT-2019-0351`
`dfn-cert: DFN-CERT-2019-0112`
`dfn-cert: DFN-CERT-2019-0104`
`dfn-cert: DFN-CERT-2018-2316`
`dfn-cert: DFN-CERT-2018-2044`
`dfn-cert: DFN-CERT-2018-2011`

Medium (CVSS: 5.0)
NVT: Apache HTTP Server /server-info accessible (HTTP)

Summary
Requesting the URI /server-info provides a comprehensive overview of the server configuration.

Vulnerability Detection Result
`Vulnerable URL: http://13.58.47.204/server-info`

Impact
Requesting the URI /server-info gives throughout information about the currently running Apache to an attacker.

Solution:
Solution type: Workaround
- If this feature is unused commenting out the appropriate section in the web servers configuration is recommended.
- If this feature is used restricting access to trusted clients is recommended.

Affected Software/OS
All Apache installations with an enabled 'mod_info' module.

Vulnerability Insight
server-info is a Apache HTTP Server handler provided by the 'mod_info' module and used to retrieve the server's configuration.

Vulnerability Detection Method
Checks if the /server-info page of Apache is accessible.
Details: `Apache HTTP Server /server-info accessible (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.10678
Version used: `2022-01-13T16:09:14Z`

References
`url: https://httpd.apache.org/docs/current/mod/mod_info.html`

Medium (CVSS: 5.3)
NVT: Apache HTTP Server /server-status accessible (HTTP)

Summary
Requesting the URI /server-status provides information on the server activity and performance.

Vulnerability Detection Result
`Vulnerable URL: http://13.58.47.204/server-status`

Impact
. . . continues on next page . . .

... continued from previous page ...

Requesting the URI /server-status gives throughout information about the currently running Apache to an attacker.

Solution:
Solution type: Mitigation
- If this feature is unused commenting out the appropriate section in the web servers configuration is recommended
- If this feature is used restricting access to trusted clients is recommended
- If the FreedomBox software is running on the target update the software to a later version

Affected Software/OS
- All Apache installations with an enabled 'mod_status' module
- FreedomBox through 20.13

Vulnerability Insight
server-status is a Apache HTTP Server handler provided by the 'mod_status' module and used to retrieve the server's activity and performance.

Vulnerability Detection Method
Checks if the /server-status page of Apache is accessible.
Details: `Apache HTTP Server /server-status accessible (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.10677
Version used: `2022-01-13T16:09:14Z`

References
`cve: CVE-2020-25073`
`url: https://httpd.apache.org/docs/current/mod/mod_status.html`

Medium (CVSS: 5.0)
NVT: Enabled Directory Listing Detection

Summary
The script attempts to identify directories with an enabled directory listing.

Vulnerability Detection Result
```
The following directories with an enabled directory listing were identified:
http://13.58.47.204/dashboard/docs
http://13.58.47.204/xampp
Please review the content manually.
```

Impact
Based on the information shown an attacker might be able to gather additional info about the structure of this application.

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: Mitigation
If not needed disable the directory listing within the webservers config.

Affected Software/OS
Webservers with an enabled directory listing.

Vulnerability Detection Method
Check the detected directories if a directory listing is enabled.
Details: `Enabled Directory Listing Detection`
OID:1.3.6.1.4.1.25623.1.0.111074
Version used: `2020-08-24T15:18:35Z`

References
`url: https://www.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities_-_D`
`↪irectory_Indexing`

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Vulnerability Detection Result
`The web server has the following HTTP methods enabled: TRACE`

Impact
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution:
Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

Affected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.

... continues on next page ...

... continued from previous page ...

Details: HTTP Debugging Methods (TRACE/TRACK) Enabled
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: 2022-05-12T09:32:01Z

References

cve: CVE-2003-1567
cve: CVE-2004-2320
cve: CVE-2004-2763
cve: CVE-2005-3398
cve: CVE-2006-4683
cve: CVE-2007-3008
cve: CVE-2008-7253
cve: CVE-2009-2823
cve: CVE-2010-0386
cve: CVE-2012-2223
cve: CVE-2014-7883
url: http://www.kb.cert.org/vuls/id/288308
url: http://www.securityfocus.com/bid/11604
url: http://www.securityfocus.com/bid/15222
url: http://www.securityfocus.com/bid/19915
url: http://www.securityfocus.com/bid/24456
url: http://www.securityfocus.com/bid/33374
url: http://www.securityfocus.com/bid/36956
url: http://www.securityfocus.com/bid/36990
url: http://www.securityfocus.com/bid/37995
url: http://www.securityfocus.com/bid/9506
url: http://www.securityfocus.com/bid/9561
url: http://www.kb.cert.org/vuls/id/867593
url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac
↪e-verbs/ba-p/784482
url: https://owasp.org/www-community/attacks/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020

Medium (CVSS: 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.

Vulnerability Detection Result

Installed version: 1.10.2
Fixed version: 3.5.0

... continues on next page ...

... continued from previous page ...

```
Installation
path / port:        //code.jquery.com
```

Solution:
Solution type: VendorFix
Update to version 3.5.0 or later.

Affected Software/OS
jQuery versions 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: `2021-07-13T02:01:14Z`

References

```
cve: CVE-2020-11023
url: https://github.com/jquery/jquery/security/advisories/GHSA-jpcq-cgw6-v4j6
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-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
```

... continues on next page ...

... continued from previous page ...

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.

Vulnerability Detection Result
Installed version: 1.10.2
Fixed version: 3.5.0
Installation
path / port: //code.jquery.com

Solution:
Solution type: VendorFix
Update to version 3.5.0 or later.

Affected Software/OS
jQuery versions 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: 2021-07-13T02:01:14Z

References

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2020-11022
url: https://github.com/jquery/jquery/security/advisories/GHSA-gxr4-xjj5-5px2
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-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
```

... continues on next page ...

... continued from previous page ...

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 1.4.2 <= 1.11.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability via vectors related to use of the text method inside after.

Vulnerability Detection Result
Installed version: 1.10.2
Fixed version: 1.11.1
Installation
path / port: //code.jquery.com

Solution:
Solution type: VendorFix
Update to version 1.11.1 or later.

Affected Software/OS
jQuery version 1.4.2 through 1.11.0.

Vulnerability Insight
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery 1.4.2 <= 1.11.0 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.150660
Version used: 2021-06-14T19:22:43Z

References
cve: CVE-2014-6071
url: https://seclists.org/fulldisclosure/2014/Sep/10

Medium (CVSS: 6.1)
NVT: jQuery < 3.0.0 XSS Vulnerability

Summary

... continues on next page ...

... continued from previous page ...

jQuery is vulnerable to Cross-site Scripting (XSS) attacks.

Vulnerability Detection Result
Installed version: 1.10.2
Fixed version: 3.0.0
Installation
path / port: //code.jquery.com

Solution:
Solution type: VendorFix
Update to version 3.0.0 or later or apply the patch.

Affected Software/OS
jQuery prior to version 3.0.0.

Vulnerability Insight
When a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery < 3.0.0 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141635
Version used: 2021-06-11T08:43:18Z

References
cve: CVE-2015-9251
url: https://github.com/jquery/jquery/issues/2432
cert-bund: CB-K22/0045
cert-bund: CB-K20/1030
cert-bund: CB-K20/0309
cert-bund: CB-K20/0041
cert-bund: CB-K19/0911
cert-bund: CB-K19/0909
cert-bund: CB-K19/0615
cert-bund: CB-K19/0321
cert-bund: CB-K19/0313
cert-bund: CB-K19/0054
cert-bund: CB-K19/0052
cert-bund: CB-K19/0049
cert-bund: CB-K19/0048
cert-bund: CB-K19/0046
cert-bund: CB-K18/1006
dfn-cert: DFN-CERT-2020-2423
dfn-cert: DFN-CERT-2020-2130
dfn-cert: DFN-CERT-2020-0630

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-0590
dfn-cert: DFN-CERT-2020-0318
dfn-cert: DFN-CERT-2019-2158
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0777
dfn-cert: DFN-CERT-2019-0772
dfn-cert: DFN-CERT-2019-0119
dfn-cert: DFN-CERT-2019-0111
dfn-cert: DFN-CERT-2018-2103
dfn-cert: DFN-CERT-2018-1163

Medium (CVSS: 6.1)
NVT: jQuery < 3.4.0 Object Extensions Vulnerability

Summary
jQuery is prone to multiple vulnerabilities regarding property injection in Object.prototype.

Vulnerability Detection Result
Installed version: 1.10.2
Fixed version: 3.4.0
Installation
path / port: //code.jquery.com

Solution:
Solution type: VendorFix
Update to version 3.4.0 or later. Patch diffs are available for older versions.

Affected Software/OS
jQuery prior to version 3.4.0.

Vulnerability Insight
jQuery is prone to multiple vulnerabilities:
- CVE-2019-5428: A prototype pollution vulnerability exists that allows an attacker to inject properties on Object.prototype.
- CVE-2019-11358: jQuery mishandles jQuery.extend(true, }}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery < 3.4.0 Object Extensions Vulnerability
OID:1.3.6.1.4.1.25623.1.0.142314
Version used: 2021-08-31T13:01:28Z

References
cve: CVE-2019-5428

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2019-11358
url: https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/
url: https://github.com/DanielRuf/snyk-js-jquery-174006?files=1
cert-bund: CB-K22/0045
cert-bund: CB-K21/1083
cert-bund: CB-K20/1049
cert-bund: CB-K20/1030
cert-bund: CB-K20/0800
cert-bund: CB-K20/0710
cert-bund: CB-K20/0324
cert-bund: CB-K20/0314
cert-bund: CB-K20/0309
cert-bund: CB-K20/0106
cert-bund: CB-K20/0041
cert-bund: CB-K20/0037
cert-bund: CB-K20/0034
cert-bund: CB-K19/0921
cert-bund: CB-K19/0920
cert-bund: CB-K19/0916
cert-bund: CB-K19/0911
cert-bund: CB-K19/0909
cert-bund: CB-K19/0619
cert-bund: CB-K19/0504
cert-bund: CB-K19/0329
dfn-cert: DFN-CERT-2021-1536
dfn-cert: DFN-CERT-2021-1503
dfn-cert: DFN-CERT-2021-0826
dfn-cert: DFN-CERT-2020-2423
dfn-cert: DFN-CERT-2020-2335
dfn-cert: DFN-CERT-2020-2286
dfn-cert: DFN-CERT-2020-2130
dfn-cert: DFN-CERT-2020-1812
dfn-cert: DFN-CERT-2020-1574
dfn-cert: DFN-CERT-2020-1537
dfn-cert: DFN-CERT-2020-1506
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2020-0769
dfn-cert: DFN-CERT-2020-0721
dfn-cert: DFN-CERT-2020-0276
dfn-cert: DFN-CERT-2020-0102
dfn-cert: DFN-CERT-2020-0100
dfn-cert: DFN-CERT-2019-2169
dfn-cert: DFN-CERT-2019-2158
dfn-cert: DFN-CERT-2019-2156
dfn-cert: DFN-CERT-2019-2126
dfn-cert: DFN-CERT-2019-1861
dfn-cert: DFN-CERT-2019-1663
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2019-1460
dfn-cert: DFN-CERT-2019-1182
dfn-cert: DFN-CERT-2019-1153
dfn-cert: DFN-CERT-2019-1118
dfn-cert: DFN-CERT-2019-1033
dfn-cert: DFN-CERT-2019-0914
dfn-cert: DFN-CERT-2019-0899
dfn-cert: DFN-CERT-2019-0805

Medium (CVSS: 5.9)
NVT: OpenSSL: 0-byte record padding oracle (CVE-2019-1559) (Windows)

Product detection result
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary
OpenSSL is prone to a padding oracle attack.

Vulnerability Detection Result
Installed version: 1.0.2j
Fixed version: 1.0.2r
Installation
path / port: 80/tcp

Impact
If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data.
In order for this to be exploitable 'non-stitched' ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). AEAD ciphersuites are not impacted.

Solution:
Solution type: VendorFix
Upgrade OpenSSL to version 1.0.2r or later. See the references for more details.

Affected Software/OS
OpenSSL versions 1.0.2-1.0.2q.
This issue does not impact OpenSSL 1.1.1 or 1.1.0.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSL: 0-byte record padding oracle (CVE-2019-1559) (Windows)`
OID:1.3.6.1.4.1.25623.1.0.108555
Version used: `2022-03-28T03:06:01Z`

Product Detection Result
Product: `cpe:/a:openssl:openssl:1.0.2j`
Method: `OpenSSL Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
`cve: CVE-2019-1559`
`url: https://www.openssl.org/news/secadv/20190226.txt`
`url: https://github.com/RUB-NDS/TLS-Padding-Oracles#openssl-cve-2019-1559`
`cert-bund: CB-K22/0045`
`cert-bund: CB-K20/0041`
`cert-bund: CB-K19/0911`
`cert-bund: CB-K19/0639`
`cert-bund: CB-K19/0623`
`cert-bund: CB-K19/0622`
`cert-bund: CB-K19/0620`
`cert-bund: CB-K19/0619`
`cert-bund: CB-K19/0615`
`cert-bund: CB-K19/0332`
`cert-bund: CB-K19/0320`
`cert-bund: CB-K19/0319`
`cert-bund: CB-K19/0173`
`dfn-cert: DFN-CERT-2020-2189`
`dfn-cert: DFN-CERT-2020-0092`
`dfn-cert: DFN-CERT-2020-0048`
`dfn-cert: DFN-CERT-2019-2457`
`dfn-cert: DFN-CERT-2019-2158`
`dfn-cert: DFN-CERT-2019-2157`
`dfn-cert: DFN-CERT-2019-2046`
`dfn-cert: DFN-CERT-2019-1996`
`dfn-cert: DFN-CERT-2019-1897`
`dfn-cert: DFN-CERT-2019-1755`
`dfn-cert: DFN-CERT-2019-1746`
`dfn-cert: DFN-CERT-2019-1722`
`dfn-cert: DFN-CERT-2019-1678`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2019-1677
dfn-cert: DFN-CERT-2019-1617
dfn-cert: DFN-CERT-2019-1486
dfn-cert: DFN-CERT-2019-1460
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-1453
dfn-cert: DFN-CERT-2019-1450
dfn-cert: DFN-CERT-2019-1408
dfn-cert: DFN-CERT-2019-1240
dfn-cert: DFN-CERT-2019-0781
dfn-cert: DFN-CERT-2019-0775
dfn-cert: DFN-CERT-2019-0771
dfn-cert: DFN-CERT-2019-0566
dfn-cert: DFN-CERT-2019-0556
dfn-cert: DFN-CERT-2019-0412
```

Medium (CVSS: 5.9)
NVT: OpenSSL: BN_mod_exp may produce incorrect results on MIPS (CVE-2021-4160) - Windows

Product detection result

```
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
```

Summary

OpenSSL is prone to a carry propagation vulnerability.

Vulnerability Detection Result

```
Installed version: 1.0.2j
Fixed version:     1.1.1m
Installation
path / port:       80/tcp
```

Solution:

Solution type: VendorFix

Update to version 1.1.1m, 3.0.1 or later.

Affected Software/OS

OpenSSL version 1.0.2, 1.1.1 and 3.0.0.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSL: BN_mod_exp may produce incorrect results on MIPS (CVE-2021-4160) - Win.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.147537
Version used: `2022-02-09T03:04:00Z`

Product Detection Result
Product: `cpe:/a:openssl:openssl:1.0.2j`
Method: `OpenSSL Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
`cve: CVE-2021-4160`
`url: https://www.openssl.org/news/secadv/20220128.txt`
`cert-bund: CB-K22/0466`
`cert-bund: CB-K22/0123`
`dfn-cert: DFN-CERT-2022-0879`
`dfn-cert: DFN-CERT-2022-0610`

Medium (CVSS: 6.5)
NVT: OpenSSL DoS Vulnerability (20180327) - Windows

Product detection result
`cpe:/a:openssl:openssl:1.0.2j`
`Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)`

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

Vulnerability Detection Result
`Installed version: 1.0.2j`
`Fixed version: 1.0.2o`
`Installation`

... continues on next page ...

... continued from previous page ...

path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 1.0.2o, 1.1.0h or later.

Affected Software/OS
OpenSSL version 1.0.2b through 1.0.2n and 1.1.0 through 1.1.0g.

Vulnerability Insight
Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Reported by OSS-fuzz.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSL DoS Vulnerability (20180327) - Windows
OID:1.3.6.1.4.1.25623.1.0.117590
Version used: 2021-08-25T12:01:03Z

Product Detection Result
Product: cpe:/a:openssl:openssl:1.0.2j
Method: OpenSSL Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
cve: CVE-2018-0739
url: https://www.openssl.org/news/secadv/20180327.txt
cert-bund: CB-K22/0045
cert-bund: CB-K21/0782
cert-bund: CB-K19/0045
cert-bund: CB-K18/1075
cert-bund: CB-K18/1012
cert-bund: CB-K18/1009
cert-bund: CB-K18/1006
cert-bund: CB-K18/1004
cert-bund: CB-K18/0808
cert-bund: CB-K18/0800
cert-bund: CB-K18/0799
cert-bund: CB-K18/0795
cert-bund: CB-K18/0794
cert-bund: CB-K18/0791
cert-bund: CB-K18/0790
cert-bund: CB-K18/0636

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K18/0606
cert-bund: CB-K18/0545
dfn-cert: DFN-CERT-2021-1541
dfn-cert: DFN-CERT-2020-0403
dfn-cert: DFN-CERT-2019-1996
dfn-cert: DFN-CERT-2019-1722
dfn-cert: DFN-CERT-2019-1398
dfn-cert: DFN-CERT-2019-1285
dfn-cert: DFN-CERT-2019-1108
dfn-cert: DFN-CERT-2019-0351
dfn-cert: DFN-CERT-2019-0112
dfn-cert: DFN-CERT-2018-2210
dfn-cert: DFN-CERT-2018-2113
dfn-cert: DFN-CERT-2018-2109
dfn-cert: DFN-CERT-2018-2103
dfn-cert: DFN-CERT-2018-1931
dfn-cert: DFN-CERT-2018-1832
dfn-cert: DFN-CERT-2018-1726
dfn-cert: DFN-CERT-2018-1411
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2018-1407
dfn-cert: DFN-CERT-2018-1402
dfn-cert: DFN-CERT-2018-1326
dfn-cert: DFN-CERT-2018-0985
dfn-cert: DFN-CERT-2018-0816
dfn-cert: DFN-CERT-2018-0725
dfn-cert: DFN-CERT-2018-0655
dfn-cert: DFN-CERT-2018-0584
```

Medium (CVSS: 5.9)
NVT: OpenSSL: EDIPARTYNAME NULL Pointer De-reference Vulnerability (CVE-2020-1971) (Windows)

Product detection result

```
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
```

Summary

OpenSSL is prone to a Denial-of-Service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.0.2j
Fixed version:     1.0.2x / 1.1.1i
Installation
path / port:       80/tcp
```

... continues on next page ...

... continued from previous page ...

Impact
An attacker may trigger a crash and cause a DoS.

Solution:
Solution type: VendorFix
OpenSSL 1.1.1 users should upgrade to 1.1.1i.
OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2x. Other users should upgrade to OpenSSL 1.1.1i.

Affected Software/OS
All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue.
OpenSSL 1.1.0 is out of support and no longer receiving updates of any kind. The impact of this issue on OpenSSL 1.1.0 has not been analysed.

Vulnerability Insight
The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack.
OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes:
1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate
2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token)
If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur.
Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the '-crl_download' option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools.
Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSL: EDIPARTYNAME NULL Pointer De-reference Vulnerability (CVE-2020-1971) (.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.117062
Version used: `2021-07-28T02:00:54Z`

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:openssl:openssl:1.0.2j
Method: OpenSSL Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
cve: CVE-2020-1971
url: https://www.openssl.org/news/secadv/20201208.txt
cert-bund: CB-K21/1065
cert-bund: CB-K21/0788
cert-bund: CB-K21/0615
cert-bund: CB-K21/0421
cert-bund: CB-K21/0111
cert-bund: CB-K21/0062
cert-bund: CB-K21/0006
cert-bund: CB-K20/1217
dfn-cert: DFN-CERT-2022-1215
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2021-2190
dfn-cert: DFN-CERT-2021-2126
dfn-cert: DFN-CERT-2021-1504
dfn-cert: DFN-CERT-2021-1225
dfn-cert: DFN-CERT-2021-0924
dfn-cert: DFN-CERT-2021-0862
dfn-cert: DFN-CERT-2021-0828
dfn-cert: DFN-CERT-2021-0826
dfn-cert: DFN-CERT-2021-0821
dfn-cert: DFN-CERT-2021-0819
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2021-0408
dfn-cert: DFN-CERT-2021-0338
dfn-cert: DFN-CERT-2021-0255
dfn-cert: DFN-CERT-2021-0134
dfn-cert: DFN-CERT-2021-0131
dfn-cert: DFN-CERT-2021-0128
dfn-cert: DFN-CERT-2021-0120
dfn-cert: DFN-CERT-2021-0107
dfn-cert: DFN-CERT-2021-0078
dfn-cert: DFN-CERT-2021-0012
dfn-cert: DFN-CERT-2020-2791
dfn-cert: DFN-CERT-2020-2668

Medium (CVSS: 5.3)
NVT: OpenSSL Information Disclosure Vulnerability (20191206) - Windows

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary
OpenSSL is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 1.0.2j
Fixed version: 1.0.2u
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 1.0.2u, 1.1.1e or later.

Affected Software/OS
OpenSSL version 1.0.2 through 1.0.2t and 1.1.1 through 1.1.1d.

Vulnerability Insight
There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSL Information Disclosure Vulnerability (20191206) - Windows
OID:1.3.6.1.4.1.25623.1.0.117591
Version used: 2021-08-25T12:01:03Z

Product Detection Result
Product: cpe:/a:openssl:openssl:1.0.2j
Method: OpenSSL Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
cve: CVE-2019-1551
url: https://www.openssl.org/news/secadv/20191206.txt
cert-bund: CB-K22/0045

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K20/0711
cert-bund: CB-K20/0710
cert-bund: CB-K20/0708
cert-bund: CB-K19/1045
dfn-cert: DFN-CERT-2022-0627
dfn-cert: DFN-CERT-2021-0826
dfn-cert: DFN-CERT-2021-0379
dfn-cert: DFN-CERT-2020-2345
dfn-cert: DFN-CERT-2020-2014
dfn-cert: DFN-CERT-2020-1788
dfn-cert: DFN-CERT-2020-1729
dfn-cert: DFN-CERT-2020-1537
dfn-cert: DFN-CERT-2020-1508
dfn-cert: DFN-CERT-2020-1472
dfn-cert: DFN-CERT-2020-1078
dfn-cert: DFN-CERT-2020-0841
dfn-cert: DFN-CERT-2020-0277
dfn-cert: DFN-CERT-2020-0091
dfn-cert: DFN-CERT-2019-2581
```

Medium (CVSS: 4.7)
NVT: OpenSSL: Microarchitecture timing vulnerability in ECC scalar multiplication (CVE-2018-5407) (Windows)

Product detection result

```
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
```

Summary

OpenSSL is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 1.0.2j
Fixed version:     1.0.2q
Installation
path / port:       80/tcp
```

Impact

An attacker with sufficient access to mount local timing attacks during ECDSA signature generation could recover the private key.

Solution:

Solution type: VendorFix

Upgrade OpenSSL to version 1.0.2q, 1.1.0i or later. See the references for more details.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
OpenSSL versions 1.1.0-1.1.0h and 1.0.2-1.0.2p.

Vulnerability Insight
OpenSSL ECC scalar multiplication, used in e.g. ECDSA and ECDH, has been shown to be vulnerable to a microarchitecture timing side channel attack.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSL: Microarchitecture timing vulnerability in ECC scalar multiplication (C.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.108484
Version used: `2022-04-13T07:21:45Z`

Product Detection Result
Product: `cpe:/a:openssl:openssl:1.0.2j`
Method: `OpenSSL Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
`cve: CVE-2018-5407`
`url: https://www.openssl.org/news/secadv/20181112.txt`
`url: https://www.openssl.org/news/vulnerabilities.html`
`url: https://github.com/openssl/openssl/commit/aab7c770353b1dc4ba045938c8fb446dd`
`↪1c4531e`
`url: https://github.com/openssl/openssl/commit/b18162a7c9bbfb57112459a4d6631fa25`
`↪8fd8c0cq`
`url: http://www.securityfocus.com/bid/105897`
`url: https://eprint.iacr.org/2018/1060.pdf`
`url: https://github.com/bbbrumley/portsmash`
`url: https://www.exploit-db.com/exploits/45785/`
`cert-bund: CB-K22/0045`
`cert-bund: CB-K20/0324`
`cert-bund: CB-K20/0136`
`cert-bund: CB-K19/0696`
`cert-bund: CB-K19/0622`
`cert-bund: CB-K19/0615`
`cert-bund: CB-K19/0321`
`cert-bund: CB-K19/0320`
`cert-bund: CB-K19/0319`
`cert-bund: CB-K19/0318`
`cert-bund: CB-K19/0316`
`cert-bund: CB-K19/0314`
`cert-bund: CB-K19/0050`
`cert-bund: CB-K19/0044`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K18/1173
cert-bund: CB-K18/1065
dfn-cert: DFN-CERT-2020-0326
dfn-cert: DFN-CERT-2019-2457
dfn-cert: DFN-CERT-2019-2456
dfn-cert: DFN-CERT-2019-2046
dfn-cert: DFN-CERT-2019-1746
dfn-cert: DFN-CERT-2019-1600
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-1450
dfn-cert: DFN-CERT-2019-1240
dfn-cert: DFN-CERT-2019-0204
dfn-cert: DFN-CERT-2019-0112
dfn-cert: DFN-CERT-2018-2541
dfn-cert: DFN-CERT-2018-2539
dfn-cert: DFN-CERT-2018-2513
dfn-cert: DFN-CERT-2018-2456
dfn-cert: DFN-CERT-2018-2444
dfn-cert: DFN-CERT-2018-2396
dfn-cert: DFN-CERT-2018-2360
dfn-cert: DFN-CERT-2018-2338
```

Medium (CVSS: 5.9)
NVT: OpenSSL Montgomery Multiplication Denial of Service Vulnerability (Windows)

Product detection result

```
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
```

Summary

OpenSSL is prone to a Denial of Service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.0.2j
Fixed version:     1.0.2k
Installation
path / port:       80/tcp
```

Impact

Successful exploitation will allow a remote attacker to cause transient authentication, key negotiation failures or reproducible erroneous outcome of public-key operations with specially crafted input and also denial of service condition.

Solution:

Solution type: VendorFix

Upgrade to OpenSSL version 1.1.0c or 1.0.2k or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
OpenSSL 1.1.0 before 1.1.0c and 1.0.2 before 1.0.2k.

Vulnerability Insight
The flaw is due to a carry propagating bug in the Broadwell-specific Montgomery multiplication procedure that handles input lengths divisible by, but longer than 256 bits.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSL Montgomery Multiplication Denial of Service Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.810543
Version used: `2022-04-13T11:57:07Z`

Product Detection Result
Product: `cpe:/a:openssl:openssl:1.0.2j`
Method: `OpenSSL Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
`cve: CVE-2016-7055`
`url: https://www.openssl.org/news/secadv/20170126.txt`
`url: http://www.securityfocus.com/bid/94242`
`url: https://www.openssl.org/news/secadv/20161110.txt`
`cert-bund: CB-K22/0045`
`cert-bund: CB-K18/0296`
`cert-bund: CB-K18/0006`
`cert-bund: CB-K17/1749`
`cert-bund: CB-K17/1748`
`cert-bund: CB-K17/1709`
`cert-bund: CB-K17/1205`
`cert-bund: CB-K17/1204`
`cert-bund: CB-K17/1198`
`cert-bund: CB-K17/0896`
`cert-bund: CB-K17/0657`
`cert-bund: CB-K17/0583`
`cert-bund: CB-K17/0307`
`cert-bund: CB-K17/0289`
`cert-bund: CB-K17/0175`
`cert-bund: CB-K17/0153`
`cert-bund: CB-K16/1753`
`dfn-cert: DFN-CERT-2018-1377`
`dfn-cert: DFN-CERT-2018-0323`
`dfn-cert: DFN-CERT-2018-0011`
`dfn-cert: DFN-CERT-2017-1830`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-1827
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1244
dfn-cert: DFN-CERT-2017-1243
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2017-0925
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0608
dfn-cert: DFN-CERT-2017-0314
dfn-cert: DFN-CERT-2017-0301
dfn-cert: DFN-CERT-2017-0178
dfn-cert: DFN-CERT-2017-0156
dfn-cert: DFN-CERT-2016-1858
```

Medium (CVSS: 5.3)
NVT: OpenSSL Multiple Vulnerabilities - Nov 2017 (Windows)

Product detection result

```
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
```

Summary

OpenSSL is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.0.2j
Fixed version:     1.0.2m
Installation
path / port:       80/tcp
```

Impact

Successful exploitation will allow a remote attacker to recover keys (private or secret keys) or to cause a buffer overread which lead to erroneous display of the certificate in text format.

Solution:

Solution type: VendorFix

Upgrade to OpenSSL version 1.1.0g or 1.0.2m or later.

Affected Software/OS

OpenSSL 1.1.0 before 1.1.0g and 1.0.2 before 1.0.2m

Vulnerability Insight

Multiple flaws exist due to:

- A carry propagating bug in the x86_64 Montgomery squaring procedure.

... continues on next page ...

... continued from previous page ...

- Malformed X.509 IPAddressFamily which could cause OOB read.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSL Multiple Vulnerabilities - Nov 2017 (Windows)
OID:1.3.6.1.4.1.25623.1.0.107204
Version used: 2021-09-13T08:01:46Z

Product Detection Result
Product: cpe:/a:openssl:openssl:1.0.2j
Method: OpenSSL Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
cve: CVE-2017-3735
cve: CVE-2017-3736
url: https://www.openssl.org/news/secadv/20171102.txt
cert-bund: CB-K22/0045
cert-bund: CB-K19/0354
cert-bund: CB-K18/1075
cert-bund: CB-K18/0808
cert-bund: CB-K18/0797
cert-bund: CB-K18/0607
cert-bund: CB-K18/0605
cert-bund: CB-K18/0604
cert-bund: CB-K18/0603
cert-bund: CB-K18/0602
cert-bund: CB-K18/0482
cert-bund: CB-K18/0205
cert-bund: CB-K18/0099
cert-bund: CB-K18/0097
cert-bund: CB-K18/0096
cert-bund: CB-K18/0057
cert-bund: CB-K17/2117
cert-bund: CB-K17/1446
cert-bund: CB-K17/0267
dfn-cert: DFN-CERT-2019-1722
dfn-cert: DFN-CERT-2019-1285
dfn-cert: DFN-CERT-2019-1108
dfn-cert: DFN-CERT-2019-0228
dfn-cert: DFN-CERT-2018-2210
dfn-cert: DFN-CERT-2018-1675
dfn-cert: DFN-CERT-2018-1410
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2018-1377
dfn-cert: DFN-CERT-2018-1048

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2018-1036
dfn-cert: DFN-CERT-2018-0952
dfn-cert: DFN-CERT-2018-0736
dfn-cert: DFN-CERT-2018-0729
dfn-cert: DFN-CERT-2018-0727
dfn-cert: DFN-CERT-2018-0696
dfn-cert: DFN-CERT-2018-0673
dfn-cert: DFN-CERT-2018-0620
dfn-cert: DFN-CERT-2018-0512
dfn-cert: DFN-CERT-2018-0223
dfn-cert: DFN-CERT-2018-0106
dfn-cert: DFN-CERT-2018-0104
dfn-cert: DFN-CERT-2018-0101
dfn-cert: DFN-CERT-2018-0064
dfn-cert: DFN-CERT-2017-2211
dfn-cert: DFN-CERT-2017-1512
dfn-cert: DFN-CERT-2017-0272
```

Medium (CVSS: 5.9)
NVT: OpenSSL: Null pointer deref in X509_issuer_and_serial_hash() (CVE-2021-23841) - Windows

Product detection result

```
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
```

Summary

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

Vulnerability Detection Result

```
Installed version: 1.0.2j
Fixed version:     1.0.2y / 1.1.1j
Installation
path / port:       80/tcp
```

Impact

This vulnerability may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack.

Solution:

Solution type: VendorFix

Update to version 1.0.2y, 1.1.1j or later. See the references for more details.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

OpenSSL version 1.0.2x and prior and 1.1.1i and prior.

Vulnerability Insight
The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSL: Null pointer deref in X509_issuer_and_serial_hash() (CVE-2021-23841) -. ↪..`
OID:1.3.6.1.4.1.25623.1.0.145404
Version used: `2021-08-30T10:29:27Z`

Product Detection Result
Product: `cpe:/a:openssl:openssl:1.0.2j`
Method: `OpenSSL Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
`cve: CVE-2021-23841`
`url: https://www.openssl.org/news/secadv/20210216.txt`
`cert-bund: CB-K21/0573`
`cert-bund: CB-K21/0572`
`cert-bund: CB-K21/0565`
`cert-bund: CB-K21/0421`
`cert-bund: CB-K21/0412`
`cert-bund: CB-K21/0389`
`cert-bund: CB-K21/0185`
`dfn-cert: DFN-CERT-2022-1215`
`dfn-cert: DFN-CERT-2022-0076`
`dfn-cert: DFN-CERT-2021-2527`
`dfn-cert: DFN-CERT-2021-2394`
`dfn-cert: DFN-CERT-2021-2216`
`dfn-cert: DFN-CERT-2021-2214`
`dfn-cert: DFN-CERT-2021-2190`
`dfn-cert: DFN-CERT-2021-1803`
`dfn-cert: DFN-CERT-2021-1670`
`dfn-cert: DFN-CERT-2021-1547`
`dfn-cert: DFN-CERT-2021-1418`
`dfn-cert: DFN-CERT-2021-1132`
`dfn-cert: DFN-CERT-2021-1129`
`dfn-cert: DFN-CERT-2021-1128`
`dfn-cert: DFN-CERT-2021-0862`
`dfn-cert: DFN-CERT-2021-0821`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-0818
dfn-cert: DFN-CERT-2021-0806
dfn-cert: DFN-CERT-2021-0740
dfn-cert: DFN-CERT-2021-0408
dfn-cert: DFN-CERT-2021-0379
dfn-cert: DFN-CERT-2021-0363

Medium (CVSS: 5.3)
NVT: OpenSSL 'OOB read' Security Bypass Vulnerability (Windows)

Product detection result
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary
OpenSSL is prone to an 'OOB read' security bypass vulnerability.

Vulnerability Detection Result
Installed version: 1.0.2j
Fixed version: 1.0.2m-dev
Installation
path / port: 80/tcp

Impact
Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions, this may aid in launching further attacks.

Solution:
Solution type: VendorFix
Upgrade to OpenSSL version 1.1.0g-dev or 1.0.2m-dev or later.

Affected Software/OS
OpenSSL 1.1.0x prior to 1.1.0g-dev, 1.0.2x prior to 1.0.2m-dev, all 1.0.1x, all 0.9.8x and all 1.0.0x versions.

Vulnerability Insight
The flaw exists as OpenSSL could do a one-byte buffer overread if an X.509 certificate has a malformed IPAddressFamily extension.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSL 'OOB read' Security Bypass Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.811719
Version used: 2022-04-13T11:57:07Z

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:openssl:openssl:1.0.2j
Method: OpenSSL Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
cve: CVE-2017-3735
url: https://www.openssl.org/news/secadv/20170828.txt
url: http://www.securityfocus.com/bid/100515
url: https://www.openssl.org/news/vulnerabilities.html#y2017
cert-bund: CB-K22/0045
cert-bund: CB-K18/1075
cert-bund: CB-K18/0808
cert-bund: CB-K18/0607
cert-bund: CB-K18/0605
cert-bund: CB-K18/0602
cert-bund: CB-K18/0205
cert-bund: CB-K18/0099
cert-bund: CB-K18/0097
cert-bund: CB-K18/0096
cert-bund: CB-K18/0057
cert-bund: CB-K17/2117
cert-bund: CB-K17/1446
cert-bund: CB-K17/0267
dfn-cert: DFN-CERT-2019-1722
dfn-cert: DFN-CERT-2019-1285
dfn-cert: DFN-CERT-2019-1108
dfn-cert: DFN-CERT-2018-2210
dfn-cert: DFN-CERT-2018-1410
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2018-0736
dfn-cert: DFN-CERT-2018-0729
dfn-cert: DFN-CERT-2018-0696
dfn-cert: DFN-CERT-2018-0223
dfn-cert: DFN-CERT-2018-0106
dfn-cert: DFN-CERT-2018-0104
dfn-cert: DFN-CERT-2018-0101
dfn-cert: DFN-CERT-2018-0064
dfn-cert: DFN-CERT-2017-2211
dfn-cert: DFN-CERT-2017-1512
dfn-cert: DFN-CERT-2017-0272

Medium (CVSS: 5.9)
NVT: OpenSSL Overflow Vulnerability (20171207, 20180327) - Windows

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary
OpenSSL is prone to an overflow bug.

Vulnerability Detection Result
Installed version: 1.0.2j
Fixed version: 1.0.2n
Installation
path / port: 80/tcp

Impact
Successfully exploiting this issue would allow an attacker to derive information about the private key.

Solution:
Solution type: VendorFix
Update to version 1.0.2n, 1.1.0h or later.

Affected Software/OS
OpenSSL 1.0.2 before 1.0.2n. OpenSSL 1.1.0 before 1.1.0h.
NOTE: This issue only affects 64-bit installations.

Vulnerability Insight
The overflow bug is in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSL Overflow Vulnerability (20171207, 20180327) - Windows
OID:1.3.6.1.4.1.25623.1.0.107270
Version used: 2022-04-13T11:57:07Z

Product Detection Result
Product: cpe:/a:openssl:openssl:1.0.2j
Method: OpenSSL Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
cve: CVE-2017-3738
url: https://www.openssl.org/news/secadv/20171207.txt
url: http://www.securityfocus.com/bid/102118

... continues on next page ...

... continued from previous page ...

```
url: https://www.openssl.org/news/secadv/20180327.txt
cert-bund: CB-K22/0045
cert-bund: CB-K19/0045
cert-bund: CB-K18/1012
cert-bund: CB-K18/1009
cert-bund: CB-K18/1006
cert-bund: CB-K18/1004
cert-bund: CB-K18/0813
cert-bund: CB-K18/0808
cert-bund: CB-K18/0608
cert-bund: CB-K18/0607
cert-bund: CB-K18/0606
cert-bund: CB-K18/0605
cert-bund: CB-K18/0545
cert-bund: CB-K18/0495
cert-bund: CB-K18/0205
cert-bund: CB-K18/0096
cert-bund: CB-K18/0057
cert-bund: CB-K17/2139
cert-bund: CB-K17/2122
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2018-1402
dfn-cert: DFN-CERT-2018-1377
dfn-cert: DFN-CERT-2018-0985
dfn-cert: DFN-CERT-2018-0736
dfn-cert: DFN-CERT-2018-0729
dfn-cert: DFN-CERT-2018-0725
dfn-cert: DFN-CERT-2018-0723
dfn-cert: DFN-CERT-2018-0696
dfn-cert: DFN-CERT-2018-0673
dfn-cert: DFN-CERT-2018-0584
dfn-cert: DFN-CERT-2018-0536
dfn-cert: DFN-CERT-2018-0223
dfn-cert: DFN-CERT-2018-0101
dfn-cert: DFN-CERT-2018-0064
dfn-cert: DFN-CERT-2017-2237
dfn-cert: DFN-CERT-2017-2216
```

Medium (CVSS: 5.9)
NVT: OpenSSL Security Bypass Vulnerability - DEC 2017 (Windows)

Product detection result

```
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
```

Summary

... continues on next page ...

... continued from previous page ...

OpenSSL is prone to a security bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 1.0.2j
Fixed version:     1.0.2n
Installation
path / port:       80/tcp
```

Impact

Successfully exploiting this issue would allow an attacker to cause a denial of service.

Solution:

Solution type: VendorFix

OpenSSL 1.0.2 users should upgrade to 1.0.2n.

Affected Software/OS

OpenSSL 1.0.2: from 1.0.2b to 1.0.2m

Vulnerability Insight

When SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer.

Vulnerability Detection Method

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

Details: `OpenSSL Security Bypass Vulnerability - DEC 2017 (Windows)`

OID:1.3.6.1.4.1.25623.1.0.107268

Version used: `2022-04-13T11:57:07Z`

Product Detection Result

Product: `cpe:/a:openssl:openssl:1.0.2j`

Method: `OpenSSL Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.145462)

References

```
cve: CVE-2017-3737
url: https://www.openssl.org/news/secadv/20171207.txt
url: http://www.securityfocus.com/bid/102103
cert-bund: CB-K22/0045
cert-bund: CB-K18/0813
cert-bund: CB-K18/0808
cert-bund: CB-K18/0608
cert-bund: CB-K18/0607
cert-bund: CB-K18/0606
cert-bund: CB-K18/0605
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K18/0495
cert-bund: CB-K18/0301
cert-bund: CB-K18/0195
cert-bund: CB-K18/0096
cert-bund: CB-K18/0057
cert-bund: CB-K17/2122
dfn-cert: DFN-CERT-2018-1402
dfn-cert: DFN-CERT-2018-1377
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1068
dfn-cert: DFN-CERT-2018-0759
dfn-cert: DFN-CERT-2018-0736
dfn-cert: DFN-CERT-2018-0729
dfn-cert: DFN-CERT-2018-0725
dfn-cert: DFN-CERT-2018-0723
dfn-cert: DFN-CERT-2018-0696
dfn-cert: DFN-CERT-2018-0673
dfn-cert: DFN-CERT-2018-0536
dfn-cert: DFN-CERT-2018-0318
dfn-cert: DFN-CERT-2018-0212
dfn-cert: DFN-CERT-2018-0101
dfn-cert: DFN-CERT-2018-0064
dfn-cert: DFN-CERT-2017-2216
```

Medium (CVSS: 5.9)
NVT: OpenSSL: Timing vulnerability in DSA signature generation (CVE-2018-0734) (Windows)

Product detection result

```
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
```

Summary

OpenSSL is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 1.0.2j
Fixed version:     1.0.2q-dev
Installation
path / port:       80/tcp
```

Solution:

Solution type: VendorFix

Upgrade OpenSSL to version 1.1.0j-dev, 1.1.1a-dev, 1.0.2q-dev or manually apply the fixes via Github. See the references for more details.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
OpenSSL versions 1.1.0-1.1.0i, 1.1.1 and 1.0.2-1.0.2p.

Vulnerability Insight
The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSL: Timing vulnerability in DSA signature generation (CVE-2018-0734) (Wind.
↪..
OID:1.3.6.1.4.1.25623.1.0.112410
Version used: 2022-04-13T07:21:45Z

Product Detection Result
Product: cpe:/a:openssl:openssl:1.0.2j
Method: OpenSSL Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
cve: CVE-2018-0734
url: https://www.openssl.org/news/secadv/20181030.txt
url: http://www.securityfocus.com/bid/105758
url: https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=43e6a58d4991a4
↪51daf4891ff05a48735df871ac
url: https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=8abfe72e8c1de1
↪b95f50aa0d9134803b4d00070f
url: https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=ef11e19d1365ee
↪a2b1851e6f540a0bf365d303e7
cert-bund: CB-K22/0045
cert-bund: CB-K20/0324
cert-bund: CB-K20/0136
cert-bund: CB-K19/1121
cert-bund: CB-K19/0622
cert-bund: CB-K19/0615
cert-bund: CB-K19/0321
cert-bund: CB-K19/0320
cert-bund: CB-K19/0319
cert-bund: CB-K19/0318
cert-bund: CB-K19/0316
cert-bund: CB-K19/0314
cert-bund: CB-K19/0050
cert-bund: CB-K19/0044
cert-bund: CB-K18/1173
cert-bund: CB-K18/1039

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-0326
dfn-cert: DFN-CERT-2019-2456
dfn-cert: DFN-CERT-2019-2305
dfn-cert: DFN-CERT-2019-2046
dfn-cert: DFN-CERT-2019-1996
dfn-cert: DFN-CERT-2019-1897
dfn-cert: DFN-CERT-2019-1746
dfn-cert: DFN-CERT-2019-1617
dfn-cert: DFN-CERT-2019-1562
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-1450
dfn-cert: DFN-CERT-2019-1240
dfn-cert: DFN-CERT-2019-0782
dfn-cert: DFN-CERT-2019-0781
dfn-cert: DFN-CERT-2019-0778
dfn-cert: DFN-CERT-2019-0775
dfn-cert: DFN-CERT-2019-0772
dfn-cert: DFN-CERT-2019-0204
dfn-cert: DFN-CERT-2019-0112
dfn-cert: DFN-CERT-2019-0104
dfn-cert: DFN-CERT-2019-0103
dfn-cert: DFN-CERT-2019-0102
dfn-cert: DFN-CERT-2018-2541
dfn-cert: DFN-CERT-2018-2539
dfn-cert: DFN-CERT-2018-2513
dfn-cert: DFN-CERT-2018-2456
dfn-cert: DFN-CERT-2018-2444
dfn-cert: DFN-CERT-2018-2396
dfn-cert: DFN-CERT-2018-2360
dfn-cert: DFN-CERT-2018-2214

Medium (CVSS: 6.5)
NVT: PHP < 7.2.26 Multiple Vulnerabilities - Dec19 (Windows)

Product detection result
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 7.2.26
Installation

... continues on next page ...

... continued from previous page ...

path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 7.2.26 or later.

Affected Software/OS
PHP versions before 7.2.26.

Vulnerability Insight
PHP is prone to multiple vulnerabilities:
- Buffer underflow in bc_shift_addsub (CVE-2019-11046)
- link() silently truncates after a null byte on Windows (CVE-2019-11044)
- DirectoryIterator class silently truncates after a null byte (CVE-2019-11045)
- Use-after-free in exif parsing under memory sanitizer (CVE-2019-11050)
- Heap-buffer-overflow READ in exif (CVE-2019-11047)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.2.26 Multiple Vulnerabilities - Dec19 (Windows)
OID:1.3.6.1.4.1.25623.1.0.143277
Version used: 2021-08-30T14:01:20Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2019-11046
cve: CVE-2019-11045
cve: CVE-2019-11044
cve: CVE-2019-11050
cve: CVE-2019-11047
url: https://www.php.net/ChangeLog-7.php#7.2.26
cert-bund: CB-K20/1199
cert-bund: CB-K19/1099
dfn-cert: DFN-CERT-2020-2627
dfn-cert: DFN-CERT-2020-1964
dfn-cert: DFN-CERT-2020-0550
dfn-cert: DFN-CERT-2020-0415
dfn-cert: DFN-CERT-2020-0382
dfn-cert: DFN-CERT-2020-0339
dfn-cert: DFN-CERT-2019-2709
dfn-cert: DFN-CERT-2019-2659

Medium (CVSS: 5.3)
NVT: PHP < 7.2.28 Multiple Vulnerabilities - Feb20 (Windows)

Product detection result
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 7.2.28
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 7.2.28 or later.

Affected Software/OS
PHP versions before 7.2.28.

Vulnerability Insight
PHP is prone to multiple vulnerabilities:
- Null Pointer Dereference in PHP Session Upload Progress (CVE-2020-7062)
- Files added to tar with Phar::buildFromIterator have all-access permissions (CVE-2020-7063)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.2.28 Multiple Vulnerabilities - Feb20 (Windows)
OID:1.3.6.1.4.1.25623.1.0.143542
Version used: 2021-07-08T11:00:45Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2020-7062
cve: CVE-2020-7063
url: https://www.php.net/ChangeLog-7.php#7.2.28
cert-bund: CB-K20/0147
dfn-cert: DFN-CERT-2020-2627

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-1964
dfn-cert: DFN-CERT-2020-1438
dfn-cert: DFN-CERT-2020-0787
dfn-cert: DFN-CERT-2020-0518
dfn-cert: DFN-CERT-2020-0485
dfn-cert: DFN-CERT-2020-0341

Medium (CVSS: 5.4)
NVT: PHP < 7.2.29 Multiple Vulnerabilities - Mar20 (Windows)

Product detection result
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 7.2.29
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 7.2.29 or later.

Affected Software/OS
PHP versions before 7.2.29.

Vulnerability Insight
PHP is prone to multiple vulnerabilities:
- Use-of-uninitialized-value in exif (CVE-2020-7064)
- get_headers() silently truncates after a null byte (CVE-2020-7066)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.2.29 Multiple Vulnerabilities - Mar20 (Windows)
OID:1.3.6.1.4.1.25623.1.0.143616
Version used: 2021-07-08T11:00:45Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
Method: PHP Detection (HTTP)

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

```
cve: CVE-2020-7064
cve: CVE-2020-7066
url: https://www.php.net/ChangeLog-7.php#7.2.29
cert-bund: CB-K21/0068
cert-bund: CB-K20/1199
cert-bund: CB-K20/0239
dfn-cert: DFN-CERT-2020-2627
dfn-cert: DFN-CERT-2020-1964
dfn-cert: DFN-CERT-2020-1438
dfn-cert: DFN-CERT-2020-1202
dfn-cert: DFN-CERT-2020-0965
dfn-cert: DFN-CERT-2020-0851
dfn-cert: DFN-CERT-2020-0787
dfn-cert: DFN-CERT-2020-0554
```

Medium (CVSS: 5.3)
NVT: PHP < 7.2.31, 7.3 < 7.3.18, 7.4 < 7.4.6 Multiple DoS Vulnerabilities - May20 (Windows)

Product detection result

```
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)
```

Summary

PHP is prone to two Denial-of-Service vulnerabilities.

Vulnerability Detection Result

```
Installed version: 5.6.30
Fixed version:     7.2.31
Installation
path / port:       80/tcp
```

Solution:

Solution type: VendorFix

Update to version 7.2.31, 7.3.18, 7.4.6 or later.

Affected Software/OS

PHP versions prior 7.2.31, 7.3 prior 7.3.18 and 7.4 prior to 7.4.6.

Vulnerability Insight

The following flaws exist:

- Long filenames cause OOM and temp files to not be cleaned

... continues on next page ...

... continued from previous page ...

- Long variables in multipart/form-data cause OOM and temp files are not cleaned
leading to a Denial-of-Service condition (CVE-2019-11048).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP < 7.2.31, 7.3 < 7.3.18, 7.4 < 7.4.6 Multiple DoS Vulnerabilities - May20 (W.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.143914
Version used: `2021-07-08T11:00:45Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2019-11048`
`url: https://www.php.net/ChangeLog-7.php#7.2.31`
`url: https://www.php.net/ChangeLog-7.php#7.3.18`
`url: https://www.php.net/ChangeLog-7.php#7.4.6`
`url: https://bugs.php.net/bug.php?id=78875`
`url: https://bugs.php.net/bug.php?id=78876`
`cert-bund: CB-K20/1199`
`cert-bund: CB-K20/0467`
`dfn-cert: DFN-CERT-2020-2627`
`dfn-cert: DFN-CERT-2020-2006`
`dfn-cert: DFN-CERT-2020-1964`
`dfn-cert: DFN-CERT-2020-1438`
`dfn-cert: DFN-CERT-2020-1376`
`dfn-cert: DFN-CERT-2020-1202`
`dfn-cert: DFN-CERT-2020-1019`

Medium (CVSS: 6.5)
NVT: PHP < 7.2.34, 7.3 < 7.3.23, 7.4 < 7.4.11 Multiple Vulnerabilities - October20 (Windows)

Product detection result
`cpe:/a:php:php:5.6.30`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.6.30`
`Fixed version:     7.2.34`

... continues on next page ...

... continued from previous page ...

Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 7.2.34, 7.3.23, 7.4.11 or later.

Affected Software/OS
PHP versions prior 7.2.34, 7.3 prior 7.3.23 and 7.4 prior to 7.4.11.

Vulnerability Insight
The following vulnerabilities exist:
- Wrong ciphertext/tag in AES-CCM encryption for a 12 bytes IV (CVE-2020-7069)
- PHP parses encoded cookie names so malicious '__Host-' cookies can be sent (CVE-2020-7070)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.2.34, 7.3 < 7.3.23, 7.4 < 7.4.11 Multiple Vulnerabilities - October20 (...
OID:1.3.6.1.4.1.25623.1.0.144695
Version used: 2021-07-08T11:00:45Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2020-7069
cve: CVE-2020-7070
url: https://www.php.net/ChangeLog-7.php#7.2.34
url: https://www.php.net/ChangeLog-7.php#7.3.23
url: https://www.php.net/ChangeLog-7.php#7.4.11
cert-bund: CB-K20/0949
dfn-cert: DFN-CERT-2021-2373
dfn-cert: DFN-CERT-2021-1645
dfn-cert: DFN-CERT-2021-0380
dfn-cert: DFN-CERT-2021-0002
dfn-cert: DFN-CERT-2020-2187
dfn-cert: DFN-CERT-2020-2111

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) - Windows

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:php:php:5.6.30
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.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 7.3.26
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 7.3.26, 7.4.14, 8.0.1 or later.

Affected Software/OS
PHP versions prior to 7.3.26, 7.4.x prior to 7.4.14 and 8.0.x prior to 8.0.1.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.3.26, 7.4.x < 7.4.14, 8.0.x < 8.0.1 Filter Vulnerability (Jan 2021) - W.
↪..
OID:1.3.6.1.4.1.25623.1.0.145115
Version used: 2021-11-29T15:00:35Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
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: CB-K21/0009
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: 5.0)
NVT: PHP < 7.3.28, 7.4.x < 7.4.18 IMAP Header Injection Vulnerability (Apr 2021) - Windows

Product detection result
cpe:/a:php:php:5.6.30
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.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 7.3.28
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 7.3.28, 7.4.18 or later.

Affected Software/OS
PHP versions prior to 7.3.28 and 7.4.x through 7.4.17.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.3.28, 7.4.x < 7.4.18 IMAP Header Injection Vulnerability (Apr 2021) - W.
↪..
OID:1.3.6.1.4.1.25623.1.0.145870
Version used: 2021-05-03T08:21:47Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
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: 5.3)
NVT: PHP < 7.3.29 Multiple Vulnerabilities (Jul 2021) - Windows

Product detection result
cpe:/a:php:php:5.6.30

... continues on next page ...

... continued from previous page ...

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

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 5.6.30
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) - Windows
OID:1.3.6.1.4.1.25623.1.0.117525
Version used: 2021-10-11T08:01:31Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2021-21704
cve: CVE-2021-21705
url: https://www.php.net/ChangeLog-7.php#7.3.29
url: http://bugs.php.net/81122
url: http://bugs.php.net/76448
url: http://bugs.php.net/76449

... continues on next page ...

... continued from previous page ...

```
url: http://bugs.php.net/76450
url: http://bugs.php.net/76452
cert-bund: CB-K21/0705
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: 5.0)
NVT: PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Aug 2021) - Windows

Product detection result
cpe:/a:php:php:5.6.30
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.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 7.3.30
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 7.3.30, 7.4.23, 8.0.10 or later.

Affected Software/OS
PHP versions prior to 7.3.30, 7.4.x through 7.4.22 and 8.0.x through 8.0.9.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Aug 2021) - Windo.
↪..
OID:1.3.6.1.4.1.25623.1.0.146585
Version used: 2021-10-25T12:34:47Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
Method: PHP Detection (HTTP)

... continues on next page ...

... continued from previous page ...

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: 6.5)
NVT: PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Sep 2021) - Windows

Product detection result
cpe:/a:php:php:5.6.30
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.

Vulnerability Detection Result
Installed version: 5.6.30
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 < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Sep 2021) - Windo.
↪..
OID:1.3.6.1.4.1.25623.1.0.117695
Version used: 2021-10-25T12:34:47Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
Method: PHP Detection (HTTP)

... continues on next page ...

... continued from previous page ...

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: CB-K21/1008
dfn-cert: DFN-CERT-2021-2474
dfn-cert: DFN-CERT-2021-1994
```

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) - Windows

Product detection result

```
cpe:/a:php:php:5.6.30
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.

Vulnerability Detection Result

```
Installed version: 5.6.30
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) - Windo.` ↪..

OID:1.3.6.1.4.1.25623.1.0.147188

... continues on next page ...

... continued from previous page ...

Version used: 2021-12-02T03:03:37Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2021-21707
url: https://www.php.net/ChangeLog-7.php#7.3.33
url: https://www.php.net/ChangeLog-7.php#7.4.26
url: https://www.php.net/ChangeLog-8.php#8.0.13
url: http://bugs.php.net/79971
cert-bund: CB-K21/1213
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: 6.8)
NVT: PHP Heap Use-After-Free Vulnerability - Sep19 (Windows)

Product detection result
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a heap-based use-after-free vulnerability.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 7.1.32
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 7.1.32 or later.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

PHP versions before 7.1.32.

Vulnerability Insight
PHP is prone to a heap use-after-free in pcrelib (cmb).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Heap Use-After-Free Vulnerability - Sep19 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.108636
Version used: `2021-04-13T14:13:08Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`url: http://bugs.php.net/75457`
`url: https://www.php.net/ChangeLog-7.php#7.1.32`

Medium (CVSS: 6.8)
NVT: PHP Multiple Vulnerabilities - Sep19 (Windows)

Product detection result
`cpe:/a:php:php:5.6.30`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 5.6.30
Fixed version:     7.2.22
Installation
path / port:       80/tcp
```

Solution:
Solution type: VendorFix
Update to version 7.2.22, 7.3.9 or later.

Affected Software/OS
PHP versions before 7.2.22 and 7.3.x before 7.3.9.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
PHP is prone to multiple vulnerabilities:
- Buffer overflow in zendparse
- Cast to object confuses GC, causes crash
- Exif crash (bus error) due to wrong alignment and invalid cast
- Use-after-free in FPM master event handling

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Multiple Vulnerabilities - Sep19 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.108638
Version used: `2021-04-13T14:13:08Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`url: http://bugs.php.net/78363`
`url: http://bugs.php.net/78379`
`url: http://bugs.php.net/78333`
`url: http://bugs.php.net/77185`
`url: https://www.php.net/ChangeLog-7.php#7.3.9`
`url: https://www.php.net/ChangeLog-7.php#7.2.22`

Medium (CVSS: 6.1)
NVT: PHP 'PHAR' Error Page Reflected XSS And DoS Vulnerabilities (Windows)

Product detection result
`cpe:/a:php:php:5.6.30`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary
PHP is prone to cross site scripting (XSS) and denial of service (DoS) vulnerabilities.

Vulnerability Detection Result
`Installed version: 5.6.30`
`Fixed version: 5.6.33`
`Installation`
`path / port: 80/tcp`

Impact

... continues on next page ...

... continued from previous page ...

Successfully exploiting this issue allows attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks and will also lead to a denial of service and exhausting the server resources.

Solution:
Solution type: VendorFix
Update to PHP version 5.6.33, 7.0.27, 7.1.13 or 7.2.1 or later.

Affected Software/OS
PHP versions before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1

Vulnerability Insight
Multiple flaws are due to:
- An input validation error on the PHAR 404 error page via the URI of a request for a .phar file.
- An integer signedness error in gd_gif_in.c in the GD Graphics Library (aka libgd).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP 'PHAR' Error Page Reflected XSS And DoS Vulnerabilities (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812732
Version used: `2021-08-10T15:24:26Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2018-5712`
`cve: CVE-2018-5711`
`url: http://php.net/ChangeLog-5.php`
`url: http://php.net/ChangeLog-7.php`
`url: https://bugs.php.net/bug.php?id=74782`
`url: https://bugs.php.net/bug.php?id=75571`
`cert-bund: CB-K20/0307`
`cert-bund: CB-K18/0498`
`cert-bund: CB-K18/0270`
`cert-bund: CB-K18/0188`
`cert-bund: CB-K18/0174`
`dfn-cert: DFN-CERT-2020-0774`
`dfn-cert: DFN-CERT-2020-0680`
`dfn-cert: DFN-CERT-2019-1737`
`dfn-cert: DFN-CERT-2019-0362`
`dfn-cert: DFN-CERT-2019-0212`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2019-0204
dfn-cert: DFN-CERT-2018-1739
dfn-cert: DFN-CERT-2018-0835
dfn-cert: DFN-CERT-2018-0733
dfn-cert: DFN-CERT-2018-0576
dfn-cert: DFN-CERT-2018-0537
dfn-cert: DFN-CERT-2018-0290
dfn-cert: DFN-CERT-2018-0205
dfn-cert: DFN-CERT-2018-0191

Medium (CVSS: 6.5)
NVT: PHP 'PHP-FPM' Denial of Service Vulnerability (Windows)

Product detection result
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

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

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 7.1.20
Installation
path / port: 80/tcp

Impact
Successfully exploitation will allow an attacker to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.

Solution:
Solution type: VendorFix
Update to PHP 7.1.20, 7.2.8 or 7.3.0alpha3.

Affected Software/OS
PHP versions 5.x up to and including 5.6.36. All 7.0.x versions, 7.1.x before 7.1.20, 7.2.x before 7.2.8 and 7.3.x before 7.3.0alpha3 on Windows.

Vulnerability Insight
The flaw exists due to the php-fpm master process restarts a child process in an endless loop when using program execution functions with a non-blocking STDIN stream.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: PHP 'PHP-FPM' Denial of Service Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.812519
Version used: 2021-06-03T02:00:18Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2015-9253
url: https://bugs.php.net/bug.php?id=73342
url: https://bugs.php.net/bug.php?id=70185
url: https://github.com/php/php-src/pull/3287
url: https://www.futureweb.at/security/CVE-2015-9253
url: https://vuldb.com//?id.113566
dfn-cert: DFN-CERT-2022-0485
dfn-cert: DFN-CERT-2022-0455
dfn-cert: DFN-CERT-2022-0431
dfn-cert: DFN-CERT-2020-0337
dfn-cert: DFN-CERT-2018-1882

Medium (CVSS: 4.7)
NVT: PHP Security Bypass Vulnerability May18 (Windows)

Product detection result
cpe:/a:php:php:5.6.30
Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
PHP is prone to a security bypass vulnerability.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 5.6.35
Installation
path / port: 80/tcp

Impact
Successful exploitation will allow an attacker to bypass security restrictions and access sensitive configuration data for other accounts directly in the PHP worker process's memory.

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Update to version 7.2.4 or 7.0.29 or 5.6.35 or 7.1.16 or later. Please see the references for more information.

Affected Software/OS
PHP versions prior to 5.6.35,
PHP versions 7.2.x prior to 7.2.4,
PHP versions 7.0.x prior to 7.0.29,
PHP versions 7.1.x prior to 7.1.16 on Windows.

Vulnerability Insight
The flaw exists as the dumpable FPM child processes allow bypassing opcache access controls

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `PHP Security Bypass Vulnerability May18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.813161
Version used: `2021-06-03T02:00:18Z`

Product Detection Result
Product: `cpe:/a:php:php:5.6.30`
Method: `PHP Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
`cve: CVE-2018-10545`
`url: http://www.php.net/ChangeLog-5.php#5.6.35`
`url: http://www.php.net/ChangeLog-7.php#7.0.29`
`url: http://www.php.net/ChangeLog-7.php#7.1.16`
`url: http://www.php.net/ChangeLog-7.php#7.2.4`
`cert-bund: CB-K18/0633`
`dfn-cert: DFN-CERT-2019-1737`
`dfn-cert: DFN-CERT-2018-1232`
`dfn-cert: DFN-CERT-2018-0920`
`dfn-cert: DFN-CERT-2018-0877`

[return to 13.58.47.204]

2.1.3 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

... continues on next page ...

... continued from previous page ...

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: 189926286
Packet 2: 189926394

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
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: 2020-08-24T08:40:10Z

References
url: http://www.ietf.org/rfc/rfc1323.txt
url: http://www.ietf.org/rfc/rfc7323.txt
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152

[return to 13.58.47.204]

2.1.4 Low 80/tcp

Low (CVSS: 3.7)
NVT: OpenSSL 1.0.2, 1.1.0, 1.1.1 Multiple Vulnerabilities - Windows

Product detection result
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)

Summary
OpenSSL is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.0.2j
Fixed version: 1.0.2t
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 1.0.2t, 1.1.0l, 1.1.1d or later.

Affected Software/OS
OpenSSL versions 1.0.2 - 1.0.2s, 1.1.0 - 1.1.0k and 1.1.1 - 1.1.1c.

Vulnerability Insight
OpenSSL is prone to multiple vulnerabilities:
- ECDSA remote timing attack (CVE-2019-1547)
- Padding Oracle in PKCS7_dataDecode and CMS_decrypt_set1_pkey (CVE-2019-1563)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSL 1.0.2, 1.1.0, 1.1.1 Multiple Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.142888
Version used: 2021-09-06T11:01:35Z

Product Detection Result
Product: cpe:/a:openssl:openssl:1.0.2j
Method: OpenSSL Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
cve: CVE-2019-1547
cve: CVE-2019-1563
url: https://www.openssl.org/news/secadv/20190910.txt
cert-bund: CB-K22/0045
cert-bund: CB-K20/1049

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K20/1016
cert-bund: CB-K20/0321
cert-bund: CB-K20/0318
cert-bund: CB-K20/0043
cert-bund: CB-K20/0038
cert-bund: CB-K20/0036
cert-bund: CB-K20/0028
cert-bund: CB-K19/1025
cert-bund: CB-K19/0919
cert-bund: CB-K19/0915
cert-bund: CB-K19/0808
dfn-cert: DFN-CERT-2020-2014
dfn-cert: DFN-CERT-2020-1729
dfn-cert: DFN-CERT-2020-0895
dfn-cert: DFN-CERT-2020-0776
dfn-cert: DFN-CERT-2020-0775
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2020-0716
dfn-cert: DFN-CERT-2020-0277
dfn-cert: DFN-CERT-2020-0101
dfn-cert: DFN-CERT-2020-0096
dfn-cert: DFN-CERT-2020-0091
dfn-cert: DFN-CERT-2020-0090
dfn-cert: DFN-CERT-2019-2164
dfn-cert: DFN-CERT-2019-2149
dfn-cert: DFN-CERT-2019-1900
```

Low (CVSS: 3.3)
NVT: OpenSSL Default Installation Paths Vulnerability (CVE-2019-1552) (Windows)

Product detection result

```
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
```

Summary

OpenSSL on Windows is prone to an insecure path defaults vulnerability.

Vulnerability Detection Result

```
Installed version: 1.0.2j
Fixed version:     Apply patch
Installation
path / port:       80/tcp
```

Solution:

Solution type: VendorFix

Apply the provided patches or update to a newer version.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
OpenSSL versions 1.0.2 through 1.0.2s, 1.1.0 through 1.1.0k and 1.1.1 through 1.1.1c.

Vulnerability Insight
OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verification in TLS. This directory is most commonly referred to as OPENSSLDIR, and is configurable with the –prefix / –openssldir configuration options.
For OpenSSL versions 1.1.0 and 1.1.1, the mingw configuration targets assume that resulting programs and libraries are installed in a Unix-like environment and the default prefix for program installation as well as for OPENSSLDIR should be '/usr/local'.
However, mingw programs are Windows programs, and as such, find themselves looking at sub-directories of 'C:/usr/local', which may be world writable, which enables untrusted users to modify OpenSSL's default configuration, insert CA certificates, modify (or even replace) existing engine modules, etc.
For OpenSSL 1.0.2, '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and Windows targets, including Visual C builds. However, some build instructions for the diverse Windows targets on 1.0.2 encourage you to specify your own –prefix.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSL Default Installation Paths Vulnerability (CVE-2019-1552) (Windows)`
OID:1.3.6.1.4.1.25623.1.0.142730
Version used: `2021-09-06T11:01:35Z`

Product Detection Result
Product: `cpe:/a:openssl:openssl:1.0.2j`
Method: `OpenSSL Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
`cve: CVE-2019-1552`
`url: https://www.openssl.org/news/secadv/20190730.txt`
`url: https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=54aa9d51b09d67`
`↪e90db443f682cface795f5af9e`
`url: https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=b15a19c148384e`
`↪73338aa7c5b12652138e35ed28`
`url: https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=d333ebaf9c7733`
`↪2754a9d5e111e2f53e1de54fdd`
`url: https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=e32bc855a81a2d`
`↪48d215c506bdeb4f598045f7e9`
`cert-bund: CB-K22/0045`
`cert-bund: CB-K20/1016`
`cert-bund: CB-K20/0321`
`cert-bund: CB-K20/0318`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K20/0043
cert-bund: CB-K20/0038
cert-bund: CB-K20/0036
cert-bund: CB-K20/0028
cert-bund: CB-K19/0919
cert-bund: CB-K19/0915
cert-bund: CB-K19/0675
dfn-cert: DFN-CERT-2020-0277
dfn-cert: DFN-CERT-2019-2164
dfn-cert: DFN-CERT-2019-2149
dfn-cert: DFN-CERT-2019-1897
dfn-cert: DFN-CERT-2019-1559
```

Low (CVSS: 3.7)
NVT: OpenSSL: Raccoon Attack (CVE-2020-1968) (Windows)

Product detection result

```
cpe:/a:openssl:openssl:1.0.2j
Detected by OpenSSL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.145462)
```

Summary

OpenSSL is prone to Racoon attacks.

Vulnerability Detection Result

```
Installed version: 1.0.2j
Fixed version:     1.0.2w
Installation
path / port:       80/tcp
```

Impact

An attacker may eavesdrop on encrypted communications sent over a TLS connection.

Solution:

Solution type: VendorFix

Update to version 1.0.2w, 1.1.1 or later.

Affected Software/OS

OpenSSL versions 1.0.2 - 1.0.2v and probably 1.1.0.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over that TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connections. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSL: Raccoon Attack (CVE-2020-1968) (Windows)`
OID:1.3.6.1.4.1.25623.1.0.144563
Version used: `2021-08-16T07:37:39Z`

Product Detection Result
Product: `cpe:/a:openssl:openssl:1.0.2j`
Method: `OpenSSL Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.145462)

References
`cve: CVE-2020-1968`
`url: https://www.openssl.org/news/secadv/20200909.txt`
`cert-bund: CB-K22/0463`
`cert-bund: CB-K22/0045`
`cert-bund: CB-K21/1090`
`cert-bund: CB-K21/0111`
`cert-bund: CB-K21/0061`
`cert-bund: CB-K20/0889`
`dfn-cert: DFN-CERT-2022-0869`
`dfn-cert: DFN-CERT-2021-2481`
`dfn-cert: DFN-CERT-2021-2187`
`dfn-cert: DFN-CERT-2021-0826`
`dfn-cert: DFN-CERT-2021-0255`
`dfn-cert: DFN-CERT-2021-0138`
`dfn-cert: DFN-CERT-2021-0134`
`dfn-cert: DFN-CERT-2020-2014`
`dfn-cert: DFN-CERT-2020-1980`

Low (CVSS: 3.6)
NVT: PHP < 7.2.33, 7.3 < 7.3.21, 7.4 < 7.4.9 DoS Vulnerability - August20 (Windows)

Product detection result
`cpe:/a:php:php:5.6.30`
`Detected by PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)`

Summary

... continues on next page ...

... continued from previous page ...

PHP is prone to a denial of service vulnerability in the phar_parse_zipfile function.

Vulnerability Detection Result
Installed version: 5.6.30
Fixed version: 7.2.33
Installation
path / port: 80/tcp

Solution:
Solution type: VendorFix
Update to version 7.2.33, 7.3.21, 7.4.9 or later.

Affected Software/OS
PHP versions prior 7.2.33, 7.3 prior 7.3.21 and 7.4 prior to 7.4.9.

Vulnerability Insight
The phar_parse_zipfile function had use-after-free vulnerability because of mishandling of the actual_alias variable.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: PHP < 7.2.33, 7.3 < 7.3.21, 7.4 < 7.4.9 DoS Vulnerability - August20 (Windows)
OID:1.3.6.1.4.1.25623.1.0.144366
Version used: 2021-07-08T11:00:45Z

Product Detection Result
Product: cpe:/a:php:php:5.6.30
Method: PHP Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.800109)

References
cve: CVE-2020-7068
url: https://www.php.net/ChangeLog-7.php#7.2.33
url: https://www.php.net/ChangeLog-7.php#7.3.21
url: https://www.php.net/ChangeLog-7.php#7.4.9
cert-bund: CB-K20/0788
dfn-cert: DFN-CERT-2021-2373
dfn-cert: DFN-CERT-2021-1645
dfn-cert: DFN-CERT-2021-1453
dfn-cert: DFN-CERT-2021-0380
dfn-cert: DFN-CERT-2020-1910
dfn-cert: DFN-CERT-2020-1732

[return to 13.58.47.204]

2.1.5 Log general/CPE-T

Log (CVSS: 0.0) NVT: CPE Inventory
Summary This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan. Note: Some CPEs for specific products might show up twice or more in the output. Background: After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.
Vulnerability Detection Result 13.58.47.204 | cpe:/a:apache:apr-util:1.5.4 13.58.47.204 | cpe:/a:apache:http_server:2.4.25 13.58.47.204 | cpe:/a:apache:portable_runtime:1.5.2 13.58.47.204 | cpe:/a:apachefriends:xampp:5.6.30 13.58.47.204 | cpe:/a:jquery:jquery:1.10.2 13.58.47.204 | cpe:/a:openssl:openssl:1.0.2j 13.58.47.204 | cpe:/a:oscommerce:oscommerce 13.58.47.204 | cpe:/a:php:php:5.6.30 13.58.47.204 | cpe:/o:microsoft:windows
Solution:
Log Method Details: CPE Inventory OID:1.3.6.1.4.1.25623.1.0.810002 Version used: 2021-04-16T10:39:13Z
References url: https://nvd.nist.gov/products/cpe

[return to 13.58.47.204]

2.1.6 Log general/tcp

Log (CVSS: 0.0) NVT: Apache HTTP Server Detection Consolidation
Summary Consolidation of Apache HTTP Server detections.
Vulnerability Detection Result
... continues on next page ...

... continued from previous page ...

```
Detected Apache HTTP Server
Version:       2.4.25
Location:      80/tcp
CPE:           cpe:/a:apache:http_server:2.4.25
Concluded from version/product identification result:
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
```

Solution:

Log Method
Details: `Apache HTTP Server Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.117232
Version used: `2021-02-25T13:36:35Z`

References
`url: https://httpd.apache.org`

Log (CVSS: 0.0)
NVT: Hostname Determination Reporting

Summary
The script reports information on how the hostname of the target was determined.

Vulnerability Detection Result

```
Hostname determination for IP 13.58.47.204:
Hostname|Source
13.58.47.204|IP-address
```

Solution:

Log Method
Details: `Hostname Determination Reporting`
OID:1.3.6.1.4.1.25623.1.0.108449
Version used: `2018-11-19T11:11:31Z`

Log (CVSS: 0.0)
NVT: jQuery Detection Consolidation

Summary
Consolidation of jQuery detections.

Vulnerability Detection Result

```
Detected jQuery
```

... continues on next page ...

... continued from previous page ...

```
Version:        1.10.2
Location:       //code.jquery.com
CPE:            cpe:/a:jquery:jquery:1.10.2
Concluded from version/product identification result:
src="//code.jquery.com/jquery-1.10.2.min.js
```

Solution:

Log Method
Details: jQuery Detection Consolidation
OID:1.3.6.1.4.1.25623.1.0.150658
Version used: 2021-09-21T07:58:23Z

References
url: https://jquery.com/

Log (CVSS: 0.0)
NVT: OpenSSL Detection Consolidation

Summary
Consolidation of OpenSSL detections.

Vulnerability Detection Result

```
Detected OpenSSL
Version:        1.0.2j
Location:       80/tcp
CPE:            cpe:/a:openssl:openssl:1.0.2j
Concluded from version/product identification result:
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
```

Solution:

Log Method
Details: OpenSSL Detection Consolidation
OID:1.3.6.1.4.1.25623.1.0.145462
Version used: 2021-07-19T12:32:02Z

References
url: https://www.openssl.org/

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

... continues on next page ...

... continued from previous page ...

Summary
This script consolidates the OS information detected by several VTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

Vulnerability Detection Result

```
Best matching OS:
OS:           Microsoft Windows
CPE:          cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (Operating System (OS) Detection (HTT
↪P))
Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.4.25 (Win32)
↪OpenSSL/1.0.2j PHP/5.6.30
Setting key "Host/runs_windows" based on this information
```

Solution:

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2022-06-09T10:10:35Z

References
url: https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: Traceroute

Summary
Collect information about the network route and network distance between the scanner host and the target host.

Vulnerability Detection Result

```
Network route from scanner (10.88.0.2) to target (13.58.47.204):
10.88.0.2
10.206.5.126
10.206.35.7
10.206.32.2
10.206.32.145
206.82.104.99
52.93.51.35
52.93.1.18
52.93.239.21
```

... continues on next page ...

... continued from previous page ...

```
52.95.1.105
52.95.1.188
15.230.39.87
15.230.39.76
108.166.248.39
108.166.248.42
108.166.248.41
13.58.47.204
Network distance between scanner and target: 17
```

Solution:

Vulnerability Insight
For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.

Log Method
A combination of the protocols ICMP and TCP is used to determine the route. This method is applicable for IPv4 only and it is also known as 'traceroute'.
Details: `Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `2021-03-12T14:25:59Z`

[return to 13.58.47.204]

2.1.7 Log 80/tcp

Log (CVSS: 0.0)
NVT: Apache APR Detection (HTTP)

Summary
HTTP based detection of Apache APR from an exposed /server-info status page.

Vulnerability Detection Result

```
Detected Apache APR-Utils
Version:       1.5.4
Location:      80/tcp
CPE:           cpe:/a:apache:apr-util:1.5.4
Concluded from version/product identification result:
Server loaded APU Version:</strong> <tt>1.5.4</tt>
Concluded from version/product identification location:
http://13.58.47.204/server-info
```

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: Apache APR Detection (HTTP)
OID:1.3.6.1.4.1.25623.1.0.111098
Version used: 2021-07-06T06:41:56Z

Log (CVSS: 0.0)
NVT: Apache APR Detection (HTTP)

Summary
HTTP based detection of Apache APR from an exposed /server-info status page.

Vulnerability Detection Result
```
Detected Apache APR
Version:       1.5.2
Location:      80/tcp
CPE:           cpe:/a:apache:portable_runtime:1.5.2
Concluded from version/product identification result:
Server loaded APR Version:</strong> <tt>1.5.2</tt>
Concluded from version/product identification location:
http://13.58.47.204/server-info
```

Solution:

Log Method
Details: Apache APR Detection (HTTP)
OID:1.3.6.1.4.1.25623.1.0.111098
Version used: 2021-07-06T06:41:56Z

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
The Hostname/IP "13.58.47.204" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 21.4.3)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://13.58.47.204/
http://13.58.47.204/cgi-bin
http://13.58.47.204/dashboard
http://13.58.47.204/dashboard/docs
http://13.58.47.204/error
http://13.58.47.204/server-info
http://13.58.47.204/server-status
http://13.58.47.204/xampp
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
The following directories were excluded from CGI scanning because the "Regex pat
↪tern to exclude directories from CGI scanning" setting of the NVT "Global vari
↪able settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\
↪.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|p
↪icture|bilder|thumbnail|media/|skins?/)"
http://13.58.47.204/dashboard/docs/images
http://13.58.47.204/dashboard/docs/images/access-phpmyadmin-remotely
http://13.58.47.204/dashboard/docs/images/activate-use-xdebug
http://13.58.47.204/dashboard/docs/images/backup-restore-mysql
http://13.58.47.204/dashboard/docs/images/configure-vhosts
http://13.58.47.204/dashboard/docs/images/configure-wildcard-subdomains
http://13.58.47.204/dashboard/docs/images/create-framework-project-zf1
http://13.58.47.204/dashboard/docs/images/create-framework-project-zf2
http://13.58.47.204/dashboard/docs/images/deploy-git-app
http://13.58.47.204/dashboard/docs/images/install-wordpress
http://13.58.47.204/dashboard/docs/images/reset-mysql-password
http://13.58.47.204/dashboard/docs/images/send-mail
http://13.58.47.204/dashboard/docs/images/transfer-files-ftp
http://13.58.47.204/dashboard/docs/images/troubleshoot-apache
http://13.58.47.204/dashboard/docs/images/use-different-php-version
```

... continues on next page ...

... continued from previous page ...

```
http://13.58.47.204/dashboard/docs/images/use-php-fcgi
http://13.58.47.204/dashboard/docs/images/use-sqlite
http://13.58.47.204/dashboard/images
http://13.58.47.204/dashboard/images/screenshots
http://13.58.47.204/dashboard/javascripts
http://13.58.47.204/dashboard/stylesheets
http://13.58.47.204/icons
http://13.58.47.204/img
Directory index found at:
http://13.58.47.204/dashboard/docs/
http://13.58.47.204/dashboard/docs/images/
http://13.58.47.204/dashboard/docs/images/access-phpmyadmin-remotely/
http://13.58.47.204/dashboard/docs/images/activate-use-xdebug/
http://13.58.47.204/dashboard/docs/images/backup-restore-mysql/
http://13.58.47.204/dashboard/docs/images/configure-vhosts/
http://13.58.47.204/dashboard/docs/images/configure-wildcard-subdomains/
http://13.58.47.204/dashboard/docs/images/create-framework-project-zf1/
http://13.58.47.204/dashboard/docs/images/create-framework-project-zf2/
http://13.58.47.204/dashboard/docs/images/deploy-git-app/
http://13.58.47.204/dashboard/docs/images/install-wordpress/
http://13.58.47.204/dashboard/docs/images/reset-mysql-password/
http://13.58.47.204/dashboard/docs/images/send-mail/
http://13.58.47.204/dashboard/docs/images/transfer-files-ftp/
http://13.58.47.204/dashboard/docs/images/troubleshoot-apache/
http://13.58.47.204/dashboard/docs/images/use-different-php-version/
http://13.58.47.204/dashboard/docs/images/use-php-fcgi/
http://13.58.47.204/dashboard/docs/images/use-sqlite/
http://13.58.47.204/xampp/
Extraneous phpinfo() script found at:
http://13.58.47.204/dashboard/phpinfo.php
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://13.58.47.204/ (mod_ssl.c [] core.c [] providers [] mod_version.c [] mod_p
↪roxy_ajp.c [] http_core.c [] mod_include.c [] mod_isapi.c [] mod_win32.c [] mo
↪d_rewrite.c [] mod_cgi.c [] mod_authz_core.c [] mod_auth_basic.c [] mod_cache_
↪disk.c [] mod_dir.c [] config [] mod_access_compat.c [] mod_dav_lock.c [] mod_
↪authz_host.c [] mod_authz_groupfile.c [] mod_mime.c [] mpm_winnt.c [] mod_so.c
↪ [] mod_allowmethods.c [] mod_proxy.c [] mod_log_config.c [] mod_actions.c []
↪mod_authn_core.c [] mod_headers.c [] mod_negotiation.c [] mod_asis.c [] mod_ph
↪p5.c [] server [] mod_status.c [] mod_info.c [] mod_autoindex.c [] mod_authn_f
↪ile.c [] mod_env.c [] mod_setenvif.c [] mod_socache_shmcb.c [] mod_alias.c []
↪hooks [] list [] mod_authz_user.c [] )
http://13.58.47.204/dashboard/docs/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
http://13.58.47.204/dashboard/docs/images/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O
↪[A] )
http://13.58.47.204/dashboard/docs/images/access-phpmyadmin-remotely/ (C=S;O [A]
↪ C=N;O [D] C=M;O [A] C=D;O [A] )
```

... continues on next page ...

... continued from previous page ...

```
http://13.58.47.204/dashboard/docs/images/activate-use-xdebug/ (C=S;O [A] C=N;O
↪[D] C=M;O [A] C=D;O [A] )
http://13.58.47.204/dashboard/docs/images/backup-restore-mysql/ (C=S;O [A] C=N;O
↪ [D] C=M;O [A] C=D;O [A] )
http://13.58.47.204/dashboard/docs/images/configure-vhosts/ (C=S;O [A] C=N;O [D]
↪ C=M;O [A] C=D;O [A] )
http://13.58.47.204/dashboard/docs/images/configure-wildcard-subdomains/ (C=S;O
↪[A] C=N;O [D] C=M;O [A] C=D;O [A] )
http://13.58.47.204/dashboard/docs/images/create-framework-project-zf1/ (C=S;O [
↪A] C=N;O [D] C=M;O [A] C=D;O [A] )
http://13.58.47.204/dashboard/docs/images/create-framework-project-zf2/ (C=S;O [
↪A] C=N;O [D] C=M;O [A] C=D;O [A] )
http://13.58.47.204/dashboard/docs/images/deploy-git-app/ (C=S;O [A] C=N;O [D] C
↪=M;O [A] C=D;O [A] )
http://13.58.47.204/dashboard/docs/images/install-wordpress/ (C=S;O [A] C=N;O [D
↪] C=M;O [A] C=D;O [A] )
http://13.58.47.204/dashboard/docs/images/reset-mysql-password/ (C=S;O [A] C=N;O
↪ [D] C=M;O [A] C=D;O [A] )
http://13.58.47.204/dashboard/docs/images/send-mail/ (C=S;O [A] C=N;O [D] C=M;O
↪[A] C=D;O [A] )
http://13.58.47.204/dashboard/docs/images/transfer-files-ftp/ (C=S;O [A] C=N;O [
↪D] C=M;O [A] C=D;O [A] )
http://13.58.47.204/dashboard/docs/images/troubleshoot-apache/ (C=S;O [A] C=N;O
↪[D] C=M;O [A] C=D;O [A] )
http://13.58.47.204/dashboard/docs/images/use-different-php-version/ (C=S;O [A]
↪C=N;O [D] C=M;O [A] C=D;O [A] )
http://13.58.47.204/dashboard/docs/images/use-php-fcgi/ (C=S;O [A] C=N;O [D] C=M
↪;O [A] C=D;O [A] )
http://13.58.47.204/dashboard/docs/images/use-sqlite/ (C=S;O [A] C=N;O [D] C=M;O
↪ [A] C=D;O [A] )
http://13.58.47.204/xampp/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
```

Solution:

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2022-03-24T09:16:49Z

References
url: https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary

... continues on next page ...

... continued from previous page ...

All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪------------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Server Banner Enumeration

Summary
This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

Vulnerability Detection Result
```
It was possible to enumerate the following HTTP server banner(s):
Server banner                                                | Enumeration technique
-------------------------------------------------------------------------------
↪-------------------------------------------
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30 | Valid HTTP 0.9 GET req
↪uest to '/index.html'
X-Powered-By: PHP/5.6.30                                     | Valid HTTP 1.1 GET req
↪uest (with extended headers) to '/index.php'
```

Solution:

Log Method
Details: HTTP Server Banner Enumeration
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: 2021-01-11T11:29:35Z

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
The remote HTTP Server banner is:
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30

Solution:

Log Method
Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2020-08-24T15:18:35Z

Log (CVSS: 0.0)
NVT: osCommerce Detection (HTTP)

Summary
HTTP based detection of osCommerce.

Vulnerability Detection Result
Detected osCommerce
Version: unknown
Location: /server-info
CPE: cpe:/a:oscommerce:oscommerce
Concluded from version/product identification location:
http://13.58.47.204/server-info/ssl_check.php

Solution:

Log Method
Details: osCommerce Detection (HTTP)
OID:1.3.6.1.4.1.25623.1.0.100001
Version used: 2021-07-22T08:27:04Z

References
url: https://www.oscommerce.com/

Log (CVSS: 0.0)
NVT: PHP Detection (HTTP)

Summary
HTTP based detection of PHP.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Detected PHP
Version:       5.6.30
Location:      80/tcp
CPE:           cpe:/a:php:php:5.6.30
Concluded from version/product identification result:
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
```

Solution:

Log Method
Details: `PHP Detection (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.800109
Version used: `2021-04-13T14:13:08Z`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A web server is running on this port`

Solution:

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2021-03-15T10:42:03Z`

Log (CVSS: 0.0)
NVT: XAMPP Detection (HTTP)

Summary
HTTP based detection of XAMPP.

Vulnerability Detection Result

```
Detected XAMPP
Version:       5.6.30
Location:      /dashboard
CPE:           cpe:/a:apachefriends:xampp:5.6.30
```

... continues on next page ...

... continued from previous page ...

Concluded from version/product identification result:
<h2>Welcome to XAMPP for Windows 5.6.30</h2>
Concluded from version/product identification location:
http://13.58.47.204/dashboard

Solution:

Log Method
Details: XAMPP Detection (HTTP)
OID:1.3.6.1.4.1.25623.1.0.900526
Version used: 2021-09-01T14:04:04Z

[return to 13.58.47.204]