Scan Report

June 7, 2023

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 “NoobBox-1”. The scan started at Mon Jun 5 09:32:38 2023 UTC and ended at Mon Jun 5 09:39:36 2023 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
192.168.64.21	17	13	2	0	0
Total: 1	17	13	2	0	0

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

This report contains all 32 results selected by the filtering described above. Before filtering there were 48 results.

2 Results per Host

2.1 192.168.64.21

Host scan start	Mon Jun 5 09:33:07 2023 UTC
Host scan end	Mon Jun 5 09:39:31 2023 UTC

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

2.1.1 High 80/tcp

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

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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: 2.4.38
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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Linux`
OID:1.3.6.1.4.1.25623.1.0.146725
Version used: `2022-08-09T10:11:17Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.38`
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
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: WID-SEC-2023-1016
cert-bund: WID-SEC-2022-1298
cert-bund: WID-SEC-2022-1189
cert-bund: WID-SEC-2022-0724
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-0190
cert-bund: CB-K22/0476
cert-bund: CB-K22/0465
cert-bund: CB-K22/0463
cert-bund: CB-K21/0992
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2022-2405
dfn-cert: DFN-CERT-2022-2167
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 <= 2.4.52 Multiple Vulnerabilities - Linux

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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: 2.4.38
Fixed version:     2.4.53
Installation
path / port:       80/tcp
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Update to version 2.4.53 or later.

Affected Software/OS
Apache HTTP Server version 2.4.52 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2022-22719: mod_lua Use of uninitialized value of in r:parsebody
- CVE-2022-22720: HTTP request smuggling vulnerability
- CVE-2022-22721: Possible buffer overflow with very large or unlimited LimitXMLRequestBody
- CVE-2022-23943: mod_sed: Read/write beyond bounds

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux`
OID:1.3.6.1.4.1.25623.1.0.113837
Version used: `2022-03-21T03:03:41Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.38`
Method: `Apache HTTP Server Detection Consolidation`
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: WID-SEC-2022-1772
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1161
cert-bund: WID-SEC-2022-1057
cert-bund: WID-SEC-2022-0898
cert-bund: WID-SEC-2022-0799
cert-bund: WID-SEC-2022-0755
cert-bund: WID-SEC-2022-0646
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0290
cert-bund: CB-K22/0619
cert-bund: CB-K22/0306
dfn-cert: DFN-CERT-2022-2799
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-2509
dfn-cert: DFN-CERT-2022-2305
dfn-cert: DFN-CERT-2022-2167
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-0899
dfn-cert: DFN-CERT-2022-0898
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0747
dfn-cert: DFN-CERT-2022-0678
dfn-cert: DFN-CERT-2022-0582
```

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

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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: 2.4.38
Fixed version:     2.4.48
Installation
path / port:       80/tcp
```

Impact

- 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 Linux.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

The following vulnerabilities exist:

- 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 - Linux`
OID:1.3.6.1.4.1.25623.1.0.112897
Version used: `2021-08-24T09:01:06Z`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.38`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References

```
cve: CVE-2020-35452
cve: CVE-2021-26690
cve: CVE-2021-26691
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: WID-SEC-2022-0438
cert-bund: WID-SEC-2022-0190
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-2022-0207
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-2021-1273
```

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

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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 buffer overflow vulnerability.

Vulnerability Detection Result

```
Installed version: 2.4.38
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 - Linux`
OID:1.3.6.1.4.1.25623.1.0.117856
Version used: `2021-12-23T12:12:57Z`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.38`
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: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1057
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-0727
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0190
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
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 2.4.32 < 2.4.44 mod_proxy_uwsgi Buffer Overflow Vulnerability (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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 buffer overflow vulnerability in mod_proxy_uwsgi.

Vulnerability Detection Result

```
Installed version: 2.4.38
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 2.4.32 to 2.4.43.

Vulnerability Insight

mod_proxy_uwsgi is prone to an information disclosure and possible remote code execution vulnerability.

. . . 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 2.4.32 < 2.4.44 mod_proxy_uwsgi Buffer Overflow Vulnerabilit.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.144374

Version used: `2021-07-22T02:00:50Z`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.38`

Method: `Apache HTTP Server Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.117232)

References

```
cve: CVE-2020-11984
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: WID-SEC-2023-1048
cert-bund: WID-SEC-2023-0063
cert-bund: CB-K21/0071
cert-bund: CB-K21/0068
cert-bund: CB-K21/0067
cert-bund: CB-K21/0059
cert-bund: CB-K20/0798
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2021-1069
dfn-cert: DFN-CERT-2021-0135
dfn-cert: DFN-CERT-2020-2628
dfn-cert: DFN-CERT-2020-2345
dfn-cert: DFN-CERT-2020-2006
dfn-cert: DFN-CERT-2020-1908
dfn-cert: DFN-CERT-2020-1854
dfn-cert: DFN-CERT-2020-1793
dfn-cert: DFN-CERT-2020-1744
```

High (CVSS: 9.8)

NVT: Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Linux

Product detection result

```
cpe:/a:apache:http_server:2.4.38
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)
```

Summary

Apache HTTP Server is prone to multiple vulnerabilities.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 2.4.38
Fixed version:     2.4.54
Installation
path / port:       80/tcp
```

Solution:
Solution type: VendorFix
Update to version 2.4.54 or later.

Affected Software/OS
Apache HTTP Server version 2.4.53 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2022-26377: mod_proxy_ajp: Possible request smuggling
- CVE-2022-28614: Read beyond bounds via ap_rwrite()
- CVE-2022-28615: Read beyond bounds in ap_strcmp_match()
- CVE-2022-29404: Denial of service in mod_lua r:parsebody
- CVE-2022-30556: Information disclosure in mod_lua with websockets
- CVE-2022-31813: mod_proxy X-Forwarded-For dropped by hop-by-hop mechanism

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Linux`
OID:1.3.6.1.4.1.25623.1.0.148252
Version used: `2022-06-20T03:04:15Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.38`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References

```
cve: CVE-2022-26377
cve: CVE-2022-28614
cve: CVE-2022-28615
cve: CVE-2022-29404
cve: CVE-2022-30556
cve: CVE-2022-31813
url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.54
cert-bund: WID-SEC-2023-0134
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2022-1767
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-1766
cert-bund: WID-SEC-2022-1764
cert-bund: WID-SEC-2022-0858
cert-bund: WID-SEC-2022-0192
cert-bund: CB-K22/0692
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2789
dfn-cert: DFN-CERT-2022-2652
dfn-cert: DFN-CERT-2022-2509
dfn-cert: DFN-CERT-2022-2310
dfn-cert: DFN-CERT-2022-2167
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1833
dfn-cert: DFN-CERT-2022-1720
dfn-cert: DFN-CERT-2022-1353
dfn-cert: DFN-CERT-2022-1296
```

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

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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 memory access vulnerability.

Vulnerability Detection Result

```
Installed version: 2.4.38
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

. . . continues on next page . . .

. . . continued from previous page . . .

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.114149
Version used: `2021-09-02T13:01:30Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.38`
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: WID-SEC-2022-0757
cert-bund: CB-K20/0708
cert-bund: CB-K19/0909
cert-bund: CB-K19/0728
dfn-cert: DFN-CERT-2022-1610
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: 8.2)
NVT: Apache HTTP Server 2.4.7 - 2.4.51 Multiple Vulnerabilities - Linux

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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: 2.4.38
Fixed version:     2.4.52
Installation
path / port:       80/tcp
```

. . . continues on next page . . .

. . . continued from previous page . . .

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.

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 - Linux`
OID:1.3.6.1.4.1.25623.1.0.117854
Version used: `2021-12-23T12:12:57Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.38`
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: WID-SEC-2022-1057
cert-bund: WID-SEC-2022-0727
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K22/0619
cert-bund: CB-K21/1296
dfn-cert: DFN-CERT-2022-2405
dfn-cert: DFN-CERT-2022-2167
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-1047
dfn-cert: DFN-CERT-2022-0872
dfn-cert: DFN-CERT-2022-0068
dfn-cert: DFN-CERT-2021-2656
```

High (CVSS: 7.8)
NVT: Apache HTTP Server < 2.4.39 Privilege Escalation Vulnerability (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.38
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)
```

Summary

In Apache HTTP Server, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

Vulnerability Detection Result

```
Installed version: 2.4.38
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 Privilege Escalation Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.142219
Version used: `2022-08-09T10:11:17Z`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.38`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References

```
cve: CVE-2019-0211
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K19/0623
cert-bund: CB-K19/0615
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K19/0267
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2019-1519
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-1238
dfn-cert: DFN-CERT-2019-1101
dfn-cert: DFN-CERT-2019-0915
dfn-cert: DFN-CERT-2019-0911
dfn-cert: DFN-CERT-2019-0815
dfn-cert: DFN-CERT-2019-0753
dfn-cert: DFN-CERT-2019-0687
dfn-cert: DFN-CERT-2019-0676
```

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

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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: 2.4.38
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 Linux.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

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 - Linux`
OID:1.3.6.1.4.1.25623.1.0.112905
Version used: `2021-08-24T06:00:58Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.38`
Method: `Apache HTTP Server Detection Consolidation`
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: 7.5)
NVT: Apache HTTP Server 2.4.20 < 2.4.44 Multiple Vulnerabilities (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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: 2.4.38
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server 2.4.20 < 2.4.44 Multiple Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.144372
Version used: `2021-07-22T02:00:50Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.38`
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: WID-SEC-2023-1048
cert-bund: WID-SEC-2023-0063
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 2.4.17 < 2.4.49 'mod_proxy' HTTP/2 Request Smuggling Vulnerability - Linux

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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: 2.4.38
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 2.4.17 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:1.3.6.1.4.1.25623.1.0.117615
Version used: `2021-09-17T11:59:51Z`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.38`
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-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: WID-SEC-2022-0722
cert-bund: CB-K21/0878
dfn-cert: DFN-CERT-2023-0497
dfn-cert: DFN-CERT-2022-2405
dfn-cert: DFN-CERT-2022-2167
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 (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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: 2.4.38
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)

. . . continues on next page . . .

. . . continued from previous page . . .

- 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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.114147
Version used: `2021-09-02T13:01:30Z`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.38`
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
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 2.4.30 < 2.4.49 DoS Vulnerability - Linux

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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 denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 2.4.38
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 2.4.30 through 2.4.48.

Vulnerability Insight
A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server 2.4.30 < 2.4.49 DoS Vulnerability - Linux`
OID:1.3.6.1.4.1.25623.1.0.146727
Version used: `2021-09-29T08:01:30Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.38`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References

```
cve: CVE-2021-36160
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: WID-SEC-2022-0724
cert-bund: CB-K21/0992
dfn-cert: DFN-CERT-2022-2405
dfn-cert: DFN-CERT-2022-2167
dfn-cert: DFN-CERT-2022-1047
dfn-cert: DFN-CERT-2021-2471
dfn-cert: DFN-CERT-2021-2034
dfn-cert: DFN-CERT-2021-1961
```

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

Product detection result

```
cpe:/a:apache:http_server:2.4.38
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)
```

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: 2.4.38
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:1.3.6.1.4.1.25623.1.0.142220

Version used: `2021-09-02T13:01:30Z`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.38`

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
```

... continues on next page ...

. . . continued from previous page . . .

```
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 < 2.4.39 mod_ssl Access Control Bypass Vulnerability (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.38
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)
```

Summary

In Apache HTTP Server a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client supporting Post-Handshake Authentication to bypass configured access control restrictions.

Vulnerability Detection Result

```
Installed version: 2.4.38
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 2.4.37 and 2.4.38.

Vulnerability Detection Method

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

Details: `Apache HTTP Server < 2.4.39 mod_ssl Access Control Bypass Vulnerability (Linux)`

OID:1.3.6.1.4.1.25623.1.0.142222

Version used: `2021-09-02T13:01:30Z`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.38`

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-2019-0215
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: CB-K20/0041
cert-bund: CB-K19/0623
cert-bund: CB-K19/0267
dfn-cert: DFN-CERT-2019-1095
dfn-cert: DFN-CERT-2019-0911
dfn-cert: DFN-CERT-2019-0676
```

High (CVSS: 7.2)
NVT: Apache HTTP Server Stack Overflow Vulnerability (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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 stack overflow vulnerability.

Vulnerability Detection Result

```
Installed version: 2.4.38
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 2.4.32 to 2.4.39.

Vulnerability Insight

When mod_remoteip was configured to use a trusted intermediary proxy server using the 'PROXY' protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer dereference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server Stack Overflow Vulnerability (Linux)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.114145
Version used: 2021-09-02T13:01:30Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.38
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References

```
cve: CVE-2019-10097
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-2020-2286
dfn-cert: DFN-CERT-2020-0716
dfn-cert: DFN-CERT-2019-2592
dfn-cert: DFN-CERT-2019-1810
dfn-cert: DFN-CERT-2019-1751
```

[return to 192.168.64.21]

2.1.2 Medium 80/tcp

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

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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: 2.4.38
Fixed version:     2.4.41
Installation
path / port:       80/tcp
```

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

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 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.114143
Version used: `2021-09-02T13:01:30Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.38`
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
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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 (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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: 2.4.38
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)
- 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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.143671

Version used: `2021-07-22T02:00:50Z`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.38`

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-2020-1927
cve: CVE-2020-1934
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-0757
cert-bund: CB-K20/1030
cert-bund: CB-K20/0708
cert-bund: CB-K20/0691
cert-bund: CB-K20/0280
dfn-cert: DFN-CERT-2022-1610
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: 5.8)
NVT: WordPress User IDs and User Names Disclosure

Summary

WordPress platforms use a parameter called ‘author’. This parameter accepts integer values and represents the ‘User ID’ of users in the web site. For example: http://www.example.com/?author=1

Vulnerability Detection Result

```
The following user names were revealed in id range 1-25.
Discovered username 'noobbox' with id '1 via URL http://192.168.64.21/wordpress/
↪?author=1
```

Impact

These problems trigger the following attack vectors:
1. The query response discloses whether the User ID is enabled.
2. The query response leaks (by redirection) the User Name corresponding with that User ID.

Solution:

Solution type: WillNotFix

. . . continues on next page . . .

. . . continued from previous page . . .

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

Vulnerability Insight

The problems found are:

1. User ID values are generated consecutively.

2. When a valid User ID is found, WordPress redirects to a web page with the name of the author.

Vulnerability Detection Method

Details: `WordPress User IDs and User Names Disclosure`

OID:1.3.6.1.4.1.25623.1.0.103222

Version used: `2023-03-01T10:20:04Z`

References

```
url: http://www.talsoft.com.ar/index.php/research/security-advisories/wordpress-
↪user-id-and-user-name-disclosure
```

Medium (CVSS: 5.3)

NVT: Apache HTTP Server < 2.4.39 mod_http2 Use-After-Free Vulnerability (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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: 2.4.38
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

. . . continues on next page . . .

. . . continued from previous page . . .

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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.142226

Version used: `2021-09-02T13:01:30Z`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.38`

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
dfn-cert: DFN-CERT-2019-0676
```

Medium (CVSS: 5.3)

NVT: Apache HTTP Server 2.4.6 - 2.4.46 Tunneling Misconfiguration Vulnerability - Linux

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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: 2.4.38
Fixed version:     2.4.48
Installation
path / port:       80/tcp
```

Solution:

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Update to version 2.4.48 or later.

Affected Software/OS

Apache HTTP Server versions 2.4.6 to 2.4.46 on Linux.

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 - Li.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.112898

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

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.38`

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: WID-SEC-2022-0438
cert-bund: CB-K21/0646
dfn-cert: DFN-CERT-2021-2394
dfn-cert: DFN-CERT-2021-1273
```

Medium (CVSS: 5.3)

NVT: Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 2.4.38
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 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.142228

Version used: `2021-09-02T13:01:30Z`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.38`

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: WID-SEC-2022-0757
cert-bund: CB-K20/0708
cert-bund: CB-K19/0623
cert-bund: CB-K19/0267
dfn-cert: DFN-CERT-2022-1610
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: 5.0)
NVT: Apache HTTP Server 2.4.0 - 2.4.55 HTTP Request Smuggling Vulnerability (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.38
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)
```

Summary

Apache HTTP Server is prone to a HTTP request smuggling vulnerability.

Vulnerability Detection Result

```
Installed version: 2.4.38
Fixed version:     2.4.56
Installation
path / port:       80/tcp
```

Impact

Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning.

Solution:

Solution type: VendorFix

Update to version 2.4.56 or later.

Affected Software/OS

Apache HTTP Server versions 2.4.0 through 2.4.55.

Vulnerability Insight

Some mod_proxy configurations allow a HTTP Request Smuggling attack.

Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution.

Vulnerability Detection Method

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

Details: `Apache HTTP Server 2.4.0 - 2.4.55 HTTP Request Smuggling Vulnerability (Linux)`

OID:1.3.6.1.4.1.25623.1.0.104597

Version used: `2023-03-09T10:20:45Z`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.38`

Method: `Apache HTTP Server Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.117232)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2023-25690
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-0657
cert-bund: WID-SEC-2023-0583
dfn-cert: DFN-CERT-2023-1232
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0788
dfn-cert: DFN-CERT-2023-0658
dfn-cert: DFN-CERT-2023-0546
```

Medium (CVSS: 5.0)
NVT: Apache HTTP Server < 2.4.55 Multiple Vulnerabilities (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.38
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: 2.4.38
Fixed version:     2.4.55
Installation
path / port:       80/tcp
```

Solution:

Solution type: VendorFix
Update to version 2.4.55 or later.

Affected Software/OS

Apache HTTP Server version 2.4.54 and prior.

Vulnerability Insight

The following vulnerabilities exist:

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

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server < 2.4.55 Multiple Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.149152
Version used: `2023-01-18T10:11:02Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.38`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References

```
cve: CVE-2006-20001
cve: CVE-2022-36760
cve: CVE-2022-37436
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: WID-SEC-2023-1022
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2023-0110
dfn-cert: DFN-CERT-2023-0658
dfn-cert: DFN-CERT-2023-0548
dfn-cert: DFN-CERT-2023-0497
dfn-cert: DFN-CERT-2023-0118
```

Medium (CVSS: 5.0)
NVT: Apache HTTP Server 2.4.30 - 2.4.55 HTTP Request Smuggling Vulnerability (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.38
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)
```

Summary
Apache HTTP Server is prone to a HTTP request smuggling vulnerability.

Vulnerability Detection Result

```
Installed version: 2.4.38
Fixed version:     2.4.56
Installation
path / port:       80/tcp
```

Solution:
Solution type: VendorFix
Update to version 2.4.56 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Apache HTTP Server versions 2.4.30 through 2.4.55.

Vulnerability Insight
HTTP Response Smuggling vulnerability via mod_proxy_uwsgi.
Special characters in the origin response header can truncate/split the response forwarded to the client.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server 2.4.30 - 2.4.55 HTTP Request Smuggling Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.104599
Version used: `2023-03-09T10:20:45Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.38`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References

```
cve: CVE-2023-27522
url: https://httpd.apache.org/security/vulnerabilities_24.html
cert-bund: WID-SEC-2023-0583
dfn-cert: DFN-CERT-2023-0658
dfn-cert: DFN-CERT-2023-0546
```

Medium (CVSS: 5.0)
NVT: Enabled Directory Listing/Indexing Detection (HTTP)

Summary
The script attempts to identify directories with an enabled directory listing/indexing on a remote web server.

Vulnerability Detection Result

```
The following directories with an enabled directory listing/indexing were identi
↪fied:
http://192.168.64.21/wordpress/wp-content/upgrade
http://192.168.64.21/wordpress/wp-content/uploads
http://192.168.64.21/wordpress/wp-content/uploads/2021
http://192.168.64.21/wordpress/wp-content/uploads/2021/03
http://192.168.64.21/wordpress/wp-content/uploads/2023
http://192.168.64.21/wordpress/wp-content/uploads/2023/06
http://192.168.64.21/wordpress/wp-includes
http://192.168.64.21/wordpress/wp-includes/ID3
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
http://192.168.64.21/wordpress/wp-includes/IXR
http://192.168.64.21/wordpress/wp-includes/PHPMailer
http://192.168.64.21/wordpress/wp-includes/Requests
http://192.168.64.21/wordpress/wp-includes/Requests/library
http://192.168.64.21/wordpress/wp-includes/Requests/src
http://192.168.64.21/wordpress/wp-includes/SimplePie
http://192.168.64.21/wordpress/wp-includes/SimplePie/Cache
http://192.168.64.21/wordpress/wp-includes/SimplePie/Content
http://192.168.64.21/wordpress/wp-includes/SimplePie/Decode
http://192.168.64.21/wordpress/wp-includes/SimplePie/HTTP
http://192.168.64.21/wordpress/wp-includes/SimplePie/Net
http://192.168.64.21/wordpress/wp-includes/SimplePie/Parse
http://192.168.64.21/wordpress/wp-includes/SimplePie/XML
http://192.168.64.21/wordpress/wp-includes/Text
http://192.168.64.21/wordpress/wp-includes/Text/Diff
http://192.168.64.21/wordpress/wp-includes/assets
http://192.168.64.21/wordpress/wp-includes/block-patterns
http://192.168.64.21/wordpress/wp-includes/block-supports
http://192.168.64.21/wordpress/wp-includes/certificates
http://192.168.64.21/wordpress/wp-includes/customize
http://192.168.64.21/wordpress/wp-includes/fonts
http://192.168.64.21/wordpress/wp-includes/html-api
http://192.168.64.21/wordpress/wp-includes/php-compat
http://192.168.64.21/wordpress/wp-includes/pomo
http://192.168.64.21/wordpress/wp-includes/random_compat
http://192.168.64.21/wordpress/wp-includes/rest-api
http://192.168.64.21/wordpress/wp-includes/sitemaps
http://192.168.64.21/wordpress/wp-includes/sodium_compat
http://192.168.64.21/wordpress/wp-includes/widgets
Please review the content manually.
```

Impact

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

Solution:

Solution type: Mitigation

If not needed disable the directory listing/indexing within the web servers config.

Affected Software/OS

Web servers with an enabled directory listing/indexing.

Vulnerability Detection Method

Checks previously detected directories on a remote web server if a directory listing/indexing is enabled.

Details: `Enabled Directory Listing/Indexing Detection (HTTP)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.111074
Version used: `2023-01-16T10:11:20Z`

References

```
url: https://wiki.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities_-_
↪Directory_Indexing
```

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

Summary

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

Vulnerability Detection Result

```
The following input fields where identified (URL:input name):
http://192.168.64.21/wordpress/wp-login.php:pwd
http://192.168.64.21/wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.64.
↪21%2Fwordpress%2Fwp-admin%2F&reauth=1:pwd
```

Impact

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

Solution:

Solution type: Workaround

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

Affected Software/OS

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

Vulnerability Detection Method

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2020-08-24T15:18:35Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

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

Medium (CVSS: 4.6)
NVT: WordPress 'wp-cron.php' Accessible/Enabled (HTTP) - Active Check

Summary
The remote WordPress instance might have a default setup of 'wp-cron.php' configured which could have security implications.

Vulnerability Detection Result

```
By doing the following HTTP request:
Affected URL : http://192.168.64.21/wordpress/wp-cron.php
HTTP Method  : GET
the response indicates that the system is exposing "wp-cron.php".
Note: Such systems reply with a 200 (OK), a text/html Content-Type and an empty
↪body.
Result:
HTTP/1.1 200 OK
Date: Mon, 05 Jun 2023 09:34:57 GMT
Server: Apache/2.4.38 (Debian)
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Solution:
Solution type: Mitigation
The following mitigation steps are suggested:
- Add the following to the 'wp-config.php' file of the instance:
define('DISABLE_WP_CRON', true);
- Restrict external access to 'wp-cron.php'
- Configure and enable a system cron to call 'wp-cron.php' locally via PHP instead
Please see the references for more information.

Affected Software/OS
All WordPress sides having a default setup of 'wp-cron.php' configured.

Vulnerability Insight
The following security implications might exist:

. . . continues on next page . . .

. . . continued from previous page . . .

- No CVE: A denial of service (DoS) on high traffic sites caused by WordPress executing 'wp-cron.php' multiple times a minute using an HTTP request.
- CVE-2023-22622: WordPress depends on unpredictable client visits to cause wp-cron.php execution and the resulting security updates, and the source code describes 'the scenario where a site may not receive enough visits to execute scheduled tasks in a timely manner' but neither the installation guide nor the security guide mentions this default behavior, or alerts the user about security risks on installations with very few visits.

Vulnerability Detection Method

Sends a crafted HTTP GET request and checks the response.
Details: `WordPress 'wp-cron.php' Accessible/Enabled (HTTP) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.104560
Version used: `2023-03-01T10:20:05Z`

References

```
cve: CVE-2023-22622
url: https://patchstack.com/articles/solving-unpredictable-wp-cron-problems-addr
↪essing-cve-2023-22622/
url: https://medium.com/@thecpanelguy/the-nightmare-that-is-wpcron-php-ae31c1d3a
↪e30
url: https://core.trac.wordpress.org/ticket/57159
url: https://github.com/advisories/GHSA-pmh6-cq54-943m
cert-bund: WID-SEC-2023-0023
```

Medium (CVSS: 4.2)
NVT: Apache HTTP Server < 2.4.39 mod_http2 DoS Vulnerability (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.38
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)
```

Summary

When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. A server that never enabled the h2 protocol or that only enabled it for https: and did not configure the '2Upgrade on' is unaffected by this.

Vulnerability Detection Result

```
Installed version: 2.4.38
Fixed version:     2.4.39
Installation
path / port:       80/tcp
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Update to version 2.4.39 or later.

Affected Software/OS
Apache HTTP Server version 2.4.38, 2.4.37, 2.4.35 and 2.4.34.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server < 2.4.39 mod_http2 DoS Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.142224
Version used: `2022-09-09T10:12:35Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.38`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References

```
cve: CVE-2019-0197
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-2019-1810
dfn-cert: DFN-CERT-2019-0676
```

[return to 192.168.64.21]

2.1.3 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Vulnerability Detection Result

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

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

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

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

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

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

References

```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 192.168.64.21]

2.1.4 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

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: 1658407027
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Packet 2: 1658408103
```

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:

Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

Affected Software/OS

TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: `TCP Timestamps Information Disclosure`

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: `2023-05-11T09:09:33Z`

References

```
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
```

[return to 192.168.64.21]

This file was automatically generated.