Scan Report

March 21, 2025

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Immediate scan of IP 10.0.0.112”. The scan started at Fri Mar 21 20:46:05 2025 UTC and ended at Fri Mar 21 20:59:22 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview **2**

1.1 Host Authentications 2

2 Results per Host **2**

2.1 10.0.0.112 2

2.1.1 High 53/tcp 3

2.1.2 High 80/tcp 5

2.1.3 Medium 21/tcp 18

2.1.4 Medium 80/tcp 19

2.1.5 Low general/icmp 21

2.1.6 Low general/tcp 22

2.1.7 Log 445/tcp 24

2.1.8 Log 21/tcp 26

2.1.9 Log 53/tcp 28

2.1.10 Log general/tcp 29

2.1.11 Log 139/tcp 32

2.1.12 Log 80/tcp 33

2.1.13 Log general/CPE-T 38

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.0.0.112	10	3	2	24	0
Total: 1	10	3	2	24	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 “High” are not shown.
Issues with the threat level “Medium” are not shown.
Issues with the threat level “Low” are not shown.
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 39 results selected by the filtering described above. Before filtering there were 39 results.

1.1 Host Authentications

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

2 Results per Host

2.1 10.0.0.112

Host scan start	Fri Mar 21 20:46:47 2025 UTC
Host scan end	Fri Mar 21 20:59:18 2025 UTC

Service (Port)	Threat Level
53/tcp	High
80/tcp	High
21/tcp	Medium
80/tcp	Medium
general/icmp	Low
general/tcp	Low
445/tcp	Log
21/tcp	Log

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
53/tcp	Log
general/tcp	Log
139/tcp	Log
80/tcp	Log
general/CPE-T	Log

2.1.1 High 53/tcp

High (CVSS: 7.5)
NVT: ISC BIND DoS Vulnerability (CVE-2024-11187) - Linux

Product detection result

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

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

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
Installed version: 9.18.30
Fixed version:     9.18.33
Installation
path / port:       53/tcp
```

Impact
A named instance vulnerable to this issue can be compelled to consume excessive CPU resources up to the point where exhaustion of resources effectively prevents the server from responding to other client queries. This issue is most likely to affect resolvers but could also degrade authoritative server performance.
- Authoritative servers are affected by this vulnerability.
- Resolvers are affected by this vulnerability.

Solution:
Solution type: VendorFix
Update to version 9.18.33, 9.20.5, 9.21.4, 9.18.33-S1 or later.

Affected Software/OS
ISC BIND version 9.11.37 and prior, 9.16.0 through 9.16.50, 9.18.0 through 9.18.32, 9.20.0 through 9.20.4, 9.21.0 through 9.21.3, 9.11.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.50-S1 and 9.18.11-S1 through 9.18.32-S1.

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Insight

It is possible to construct a zone such that some queries to it will generate responses containing numerous records in the Additional section. An attacker sending many such queries can cause either the authoritative server itself or an independent resolver to use disproportionate resources processing the queries. Zones will usually need to have been deliberately crafted to attack this exposure.

Vulnerability Detection Method

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

Details: `ISC BIND DoS Vulnerability (CVE-2024-11187) - Linux`

OID:1.3.6.1.4.1.25623.1.0.153891

Version used: `2025-01-31T05:37:27Z`

Product Detection Result

Product: `cpe:/a:isc:bind:9.18.30`

Method: `ISC BIND Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.145294)

References

```
cve: CVE-2024-11187
url: https://kb.isc.org/docs/cve-2024-11187
cert-bund: WID-SEC-2025-0217
dfn-cert: DFN-CERT-2025-0300
dfn-cert: DFN-CERT-2025-0269
```

High (CVSS: 7.5)

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

Product detection result

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

Summary

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

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
Installed version: 9.18.30
Fixed version:     9.18.33
Installation
path / port:       53/tcp
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

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

Solution:
Solution type: VendorFix
Update to version 9.18.33, 9.20.5, 9.21.4, 9.18.33-S1 or later.

Affected Software/OS
ISC BIND version 9.18.0 through 9.18.32, 9.20.0 through 9.20.4, 9.21.0 through 9.21.3 and 9.18.11-S1 through 9.18.32-S1.

Vulnerability Insight
Clients using DNS-over-HTTPS (DoH) can exhaust a DNS resolver's CPU and/or memory by flooding it with crafted valid or invalid HTTP/2 traffic.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ISC BIND DoS Vulnerability (CVE-2024-12705) - Linux`
OID:1.3.6.1.4.1.25623.1.0.153893
Version used: `2025-01-31T05:37:27Z`

Product Detection Result
Product: `cpe:/a:isc:bind:9.18.30`
Method: `ISC BIND Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.145294)

References
```
cve: CVE-2024-12705
url: https://kb.isc.org/docs/cve-2024-12705
cert-bund: WID-SEC-2025-0217
dfn-cert: DFN-CERT-2025-0269
```

[return to 10.0.0.112]

2.1.2 High 80/tcp

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

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

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

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
Installed version: 2.4.52
Fixed version:     2.4.53
Installation
path / port:       80/tcp
```

Solution:
Solution type: VendorFix
Update to version 2.4.53 or later.

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

Vulnerability Insight
The following vulnerabilities exist:

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

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

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

References

```
url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.53
cve: CVE-2022-22719
cve: CVE-2022-22720
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2022-22721
cve: CVE-2022-23943
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2022-1772
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1161
cert-bund: WID-SEC-2022-1057
cert-bund: WID-SEC-2022-0898
cert-bund: WID-SEC-2022-0799
cert-bund: WID-SEC-2022-0755
cert-bund: WID-SEC-2022-0646
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0290
cert-bund: CB-K22/0619
cert-bund: CB-K22/0306
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2509
dfn-cert: DFN-CERT-2022-2305
dfn-cert: DFN-CERT-2022-2167
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-0899
dfn-cert: DFN-CERT-2022-0898
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0747
dfn-cert: DFN-CERT-2022-0678
dfn-cert: DFN-CERT-2022-0582
```

High (CVSS: 9.8)
NVT: Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Linux

Product detection result

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

Summary

Apache HTTP Server is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
Installed version: 2.4.52
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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:2.4.52`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References

```
cve: CVE-2022-26377
cve: CVE-2022-28614
cve: CVE-2022-28615
cve: CVE-2022-29404
cve: CVE-2022-30556
cve: CVE-2022-31813
url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.54
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2023-1969
cert-bund: WID-SEC-2023-0134
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1766
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

High (CVSS: 9.8)
NVT: Apache HTTP Server 2.4.0 - 2.4.55 HTTP Request Smuggling Vulnerability - Linux

Product detection result

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

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

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
Installed version: 2.4.52
Fixed version:     2.4.56
Installation
path / port:       80/tcp
```

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

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

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Apache HTTP Server versions 2.4.0 through 2.4.55.

Vulnerability Insight

Some mod_proxy configurations allow a HTTP Request Smuggling attack.

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

Vulnerability Detection Method

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

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

OID:1.3.6.1.4.1.25623.1.0.104597

Version used: `2024-02-15T05:05:40Z`

Product Detection Result

Product: `cpe:/a:apache:http_server:2.4.52`

Method: `Apache HTTP Server Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.117232)

References

```
cve: CVE-2023-25690
url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.56
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-3129
cert-bund: WID-SEC-2023-2694
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1809
cert-bund: WID-SEC-2023-1807
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-0657
cert-bund: WID-SEC-2023-0583
dfn-cert: DFN-CERT-2023-1648
dfn-cert: DFN-CERT-2023-1297
dfn-cert: DFN-CERT-2023-1232
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0788
dfn-cert: DFN-CERT-2023-0658
dfn-cert: DFN-CERT-2023-0546
```

High (CVSS: 9.8)

NVT: Apache HTTP Server < 2.4.60 Multiple Vulnerabilities - Linux

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

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

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
Installed version: 2.4.52
Fixed version:     2.4.60
Installation
path / port:       80/tcp
```

Solution:
Solution type: VendorFix
Update to version 2.4.60 or later.

Affected Software/OS
Apache HTTP Server version 2.4.59 and prior.

Vulnerability Insight
The following flaws exist:
- CVE-2024-36387: Denial of Service (DoS) by Null pointer in websocket over HTTP/2
- CVE-2024-38473: Proxy encoding problem
- CVE-2024-38474: Weakness with encoded question marks in backreferences
- CVE-2024-38475: Weakness in mod_rewrite when first segment of substitution matches filesystem path
- CVE-2024-38476: May use exploitable/malicious backend application output to run local handlers via internal redirect
- CVE-2024-38477: Crash resulting in DoS in mod_proxy via a malicious request
- CVE-2024-39573: mod_rewrite proxy handler substitution

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

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

. . . continues on next page . . .

. . . continued from previous page . . .

References

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

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

Product detection result

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

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
Installed version: 2.4.52
Fixed version:     2.4.55
Installation
path / port:       80/tcp
```

Solution:
Solution type: VendorFix
Update to version 2.4.55 or later.

Affected Software/OS
Apache HTTP Server version 2.4.54 and prior.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server < 2.4.55 Multiple Vulnerabilities - Linux`
OID:1.3.6.1.4.1.25623.1.0.149152
Version used: `2024-02-15T05:05:40Z`

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

References

```
cve: CVE-2006-20001
cve: CVE-2022-36760
cve: CVE-2022-37436
url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.55
cert-bund: WID-SEC-2024-3195
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2674
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1022
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2023-0110
dfn-cert: DFN-CERT-2023-2545
dfn-cert: DFN-CERT-2023-1895
dfn-cert: DFN-CERT-2023-1297
dfn-cert: DFN-CERT-2023-0658
dfn-cert: DFN-CERT-2023-0548
dfn-cert: DFN-CERT-2023-0497
dfn-cert: DFN-CERT-2023-0118
```

High (CVSS: 7.5)
NVT: Apache HTTP Server 2.4.30 - 2.4.55 HTTP Request Smuggling Vulnerability - Linux

Product detection result

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

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

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
Installed version: 2.4.52
Fixed version:     2.4.56
Installation
path / port:       80/tcp
```

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

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

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

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server 2.4.30 - 2.4.55 HTTP Request Smuggling Vulnerability - Linux`
OID:1.3.6.1.4.1.25623.1.0.104599
Version used: `2024-02-15T05:05:40Z`

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

References

```
cve: CVE-2023-27522
url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.56
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0583
dfn-cert: DFN-CERT-2024-1808
dfn-cert: DFN-CERT-2023-1895
dfn-cert: DFN-CERT-2023-0658
dfn-cert: DFN-CERT-2023-0546
```

High (CVSS: 7.5)
NVT: Apache HTTP Server < 2.4.58 'mod_macro' Out-of-bounds Read Vulnerability - Linux

Product detection result

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

Summary
Apache HTTP Server is prone to an out-of-bounds read vulnerability in mod_macro.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
Installed version: 2.4.52
Fixed version:     2.4.58
Installation
path / port:       80/tcp
```

Solution:
Solution type: VendorFix
Update to version 2.4.58 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Apache HTTP Server version 2.4.57 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server < 2.4.58 'mod_macro' Out-of-bounds Read Vulnerability - Linux`
OID:1.3.6.1.4.1.25623.1.0.100272
Version used: `2024-02-15T05:05:40Z`

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

References

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

High (CVSS: 7.5)
NVT: Apache HTTP Server < 2.4.59 Multiple Vulnerabilities - Linux

Product detection result

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

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

. . . continues on next page . . .

. . . continued from previous page . . .

Quality of Detection (QoD): 30%

Vulnerability Detection Result

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

Solution:
Solution type: VendorFix
Update to version 2.4.59 or later.

Affected Software/OS
Apache HTTP Server version 2.4.58 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2023-38709: HTTP response splitting
- CVE-2024-24795: HTTP response splitting in multiple modules
- CVE-2024-27316: HTTP/2 DoS by memory exhaustion on endless continuation frames

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server < 2.4.59 Multiple Vulnerabilities - Linux`
OID:1.3.6.1.4.1.25623.1.0.152039
Version used: `2024-06-07T05:05:42Z`

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

References

```
cve: CVE-2023-38709
cve: CVE-2024-24795
cve: CVE-2024-27316
url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.59
url: https://kb.cert.org/vuls/id/421644
url: https://nowotarski.info/http2-continuation-flood/
url: https://nowotarski.info/http2-continuation-flood-technical-details/
cert-bund: WID-SEC-2024-1725
cert-bund: WID-SEC-2024-1643
cert-bund: WID-SEC-2024-1642
cert-bund: WID-SEC-2024-1504
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0801
cert-bund: WID-SEC-2024-0789
dfn-cert: DFN-CERT-2024-2900
dfn-cert: DFN-CERT-2024-2534
dfn-cert: DFN-CERT-2024-2076
dfn-cert: DFN-CERT-2024-1958
dfn-cert: DFN-CERT-2024-1853
dfn-cert: DFN-CERT-2024-1749
dfn-cert: DFN-CERT-2024-1697
dfn-cert: DFN-CERT-2024-1411
dfn-cert: DFN-CERT-2024-1335
dfn-cert: DFN-CERT-2024-1238
dfn-cert: DFN-CERT-2024-1031
dfn-cert: DFN-CERT-2024-1010
dfn-cert: DFN-CERT-2024-0964
dfn-cert: DFN-CERT-2024-0901
dfn-cert: DFN-CERT-2024-0890
```

[return to 10.0.0.112]

2.1.3 Medium 21/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Please specify the password.
Anonymous sessions:     331 Please specify the password.
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution:
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2023-12-20T05:05:58Z`

[return to 10.0.0.112]

2.1.4 Medium 80/tcp

Medium (CVSS: 5.9)
NVT: Apache HTTP Server 2.4.17 - 2.4.57 DoS Vulnerability - Linux

Product detection result

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

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

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
Installed version: 2.4.52
Fixed version:     2.4.58
Installation
path / port:       80/tcp
```

Solution:
Solution type: VendorFix
Update to version 2.4.58 or later.

Affected Software/OS
Apache HTTP Server version 2.4.17 through 2.4.57.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.
This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During 'normal' HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server 2.4.17 - 2.4.57 DoS Vulnerability - Linux`
OID:1.3.6.1.4.1.25623.1.0.100310
Version used: `2024-08-02T05:05:39Z`

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

References

```
cve: CVE-2023-45802
url: https://httpd.apache.org/security/vulnerabilities_24.html#2.4.58
url: https://www.openwall.com/lists/oss-security/2023/10/19/6
url: https://github.com/icing/blog/blob/main/h2-rapid-reset.md
cert-bund: WID-SEC-2024-0769
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2712
dfn-cert: DFN-CERT-2024-2968
dfn-cert: DFN-CERT-2024-1411
dfn-cert: DFN-CERT-2024-1335
dfn-cert: DFN-CERT-2024-1152
dfn-cert: DFN-CERT-2024-1010
dfn-cert: DFN-CERT-2023-3071
dfn-cert: DFN-CERT-2023-2596
dfn-cert: DFN-CERT-2023-2583
```

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

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

Quality of Detection (QoD): 30%

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
The following directories with an enabled directory listing/indexing were identi
↪fied:
http://10.0.0.112/mutillidae
Please review the content manually.
```

Impact

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

Solution:

Solution type: Mitigation

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

Affected Software/OS

Web servers with an enabled directory listing/indexing.

Vulnerability Detection Method

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

Note: This check has a low QoD (Quality of Detection) value as it is not possible to automatically determine if the directory listing/indexing has been enabled on purpose (which is also a valid use case for some software products).

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

OID:1.3.6.1.4.1.25623.1.0.111074

Version used: `2024-12-17T05:05:41Z`

References

```
cve: CVE-2023-37599
cve: CVE-2024-1076
url: https://wiki.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities_-_
↪Directory_Indexing
```

[return to 10.0.0.112]

2.1.5 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary

The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

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

Impact

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

Solution:

Solution type: Mitigation

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely

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

Vulnerability Insight

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

Vulnerability Detection Method

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: `ICMP Timestamp Reply Information Disclosure`

OID:1.3.6.1.4.1.25623.1.0.103190

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

References

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

[return to 10.0.0.112]

2.1.6 Low general/tcp

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

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 2560935009
Packet 2: 2560936100
```

Impact

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

Solution:

Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS

TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight

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

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP Timestamps Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

References

```
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[return to 10.0.0.112]

2.1.7 Log 445/tcp

Log (CVSS: 0.0)
NVT: SMB Login Successful For Authenticated Checks

Summary
It was possible to login using the provided SMB credentials. Hence authenticated checks are enabled.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution:

Log Method
Details: `SMB Login Successful For Authenticated Checks`
OID:1.3.6.1.4.1.25623.1.0.108539
Version used: `2023-07-28T16:09:07Z`

Log (CVSS: 0.0)
NVT: Microsoft Windows SMB Accessible Shares

Summary
The script detects the Windows SMB Accessible Shares and sets the result into KB.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following shares were found
IPC$
```

Solution:

Log Method
Details: `Microsoft Windows SMB Accessible Shares`
OID:1.3.6.1.4.1.25623.1.0.902425
Version used: `2023-01-31T10:08:41Z`

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
A CIFS server is running on this port
```

Solution:

Log Method

Details: `SMB/CIFS Server Detection`
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: SMB log in

Summary

This script attempts to logon into the remote host using login/password credentials.

Quality of Detection (QoD): 97%

Vulnerability Detection Result

```
It was possible to log into the remote host using the SMB protocol.
```

Solution:

Log Method

Details: `SMB log in`
OID:1.3.6.1.4.1.25623.1.0.10394
Version used: `2023-11-28T05:05:32Z`

Log (CVSS: 0.0)
NVT: SMB Remote Version Detection

Summary

Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.

Quality of Detection (QoD): 80%

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
SMBv2 and SMBv3 are enabled on remote target
```

Solution:

Log Method

Details: `SMB Remote Version Detection`
OID:1.3.6.1.4.1.25623.1.0.807830
Version used: `2023-07-26T05:05:09Z`

[return to 10.0.0.112]

2.1.8 Log 21/tcp

Log (CVSS: 0.0)
NVT: Services

Summary

This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
An FTP server is running on this port.
Here is its banner :
220 (vsFTPd 3.0.5)
```

Solution:

Vulnerability Insight

This plugin attempts to guess which service is running on the remote port(s). 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.

Log Method

Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)
NVT: FTP Banner Detection

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This script detects and reports a FTP Server Banner.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Remote FTP server banner:
220 (vsFTPd 3.0.5)
This is probably (a):
- vsFTPd
```

Solution:

Log Method

Details: `FTP Banner Detection`
OID:1.3.6.1.4.1.25623.1.0.10092
Version used: `2024-06-07T15:38:39Z`

Log (CVSS: 0.0)
NVT: vsFTPd FTP Server Detection

Summary

The script is grabbing the banner of a FTP server and attempts to identify a vsFTPd FTP Server and its version from the reply.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected vsFTPd
Version:       3.0.5
Location:      21/tcp
CPE:           cpe:/a:beasts:vsftpd:3.0.5
Concluded from version/product identification result:
220 (vsFTPd 3.0.5)
```

Solution:

Log Method

Details: `vsFTPd FTP Server Detection`
OID:1.3.6.1.4.1.25623.1.0.111050
Version used: `2023-07-26T05:05:09Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: FTP Missing Support For AUTH TLS

Summary
The remote FTP server does not support the 'AUTH TLS' command.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote FTP server does not support the 'AUTH TLS' command.
```

Solution:

Log Method
Details: `SSL/TLS: FTP Missing Support For AUTH TLS`
OID:1.3.6.1.4.1.25623.1.0.108553
Version used: `2021-03-19T08:13:38Z`

[return to 10.0.0.112]

2.1.9 Log 53/tcp

Log (CVSS: 0.0)
NVT: Check open ports

Summary
This plugin checks if the port scanners did not kill a service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by a plugin
```

Solution:

Log Method
Details: `Check open ports`
OID:1.3.6.1.4.1.25623.1.0.10919
Version used: `2023-08-03T05:05:16Z`

Log (CVSS: 0.0)
NVT: DNS Server Detection (TCP)

Summary
TCP based detection of a DNS server.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote DNS server banner is:
9.18.30-0ubuntu0.22.04.2-Ubuntu
```

Solution:

Log Method
Details: `DNS Server Detection (TCP)`
OID:1.3.6.1.4.1.25623.1.0.108018
Version used: `2021-11-30T08:05:58Z`

[return to 10.0.0.112]

2.1.10 Log general/tcp

Log (CVSS: 0.0)
NVT: Hostname Determination Reporting

Summary
The script reports information on how the hostname of the target was determined.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Hostname determination for IP 10.0.0.112:
Hostname|Source
10.0.0.112|IP-address
```

Solution:

Log Method
Details: `Hostname Determination Reporting`
OID:1.3.6.1.4.1.25623.1.0.108449
Version used: `2022-07-27T10:11:28Z`

Log (CVSS: 0.0)
NVT: ISC BIND Detection Consolidation

Summary
Consolidation of ISC BIND detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected ISC BIND
Version:       9.18.30
Location:      53/tcp
CPE:           cpe:/a:isc:bind:9.18.30
Concluded from version/product identification result:
9.18.30-0ubuntu0.22.04.2-Ubuntu
```

Solution:

Log Method
Details: `ISC BIND Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.145294
Version used: `2022-03-28T10:48:38Z`

References
`url: https://www.isc.org/bind/`

Log (CVSS: 0.0)
NVT: Apache HTTP Server Detection Consolidation

Summary
Consolidation of Apache HTTP Server detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected Apache HTTP Server
Version:       2.4.52
Location:      80/tcp
CPE:           cpe:/a:apache:http_server:2.4.52
Concluded from version/product identification result:
Server: Apache/2.4.52 (Ubuntu)
```

Solution:

Log Method

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Apache HTTP Server Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.117232
Version used: `2024-03-08T15:37:10Z`

References
`url: https://httpd.apache.org`

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

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 forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Best matching OS:
OS:           Ubuntu
CPE:          cpe:/o:canonical:ubuntu_linux
Found by VT:  1.3.6.1.4.1.25623.1.0.108014 (Operating System (OS) Detection (DNS
↪))
Concluded from DNS server banner on port 53/tcp: 9.18.30-0ubuntu0.22.04.2-Ubuntu
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS:           Linux/Unix
CPE:          cpe:/o:linux:kernel
Found by VT:  1.3.6.1.4.1.25623.1.0.105355 (Operating System (OS) Detection (FTP
↪))
Concluded from FTP banner on port 21/tcp: 220 (vsFTPd 3.0.5)
OS:           Ubuntu 22.04
Version:      22.04
CPE:          cpe:/o:canonical:ubuntu_linux:22.04
Found by VT:  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/2.4.52 (Ubuntu)
OS:           Ubuntu
CPE:          cpe:/o:canonical:ubuntu_linux
Found by VT:  1.3.6.1.4.1.25623.1.0.111067 (Operating System (OS) Detection (HTT
↪P))
Concluded from HTTP Server default page on port 80/tcp: <title>Apache2 Ubuntu De
↪fault Page
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:

Log Method
Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `2025-01-31T15:39:24Z`

References
```
url: https://forum.greenbone.net/c/vulnerability-tests/7
```

Log (CVSS: 0.0)
NVT: Traceroute

Summary
Collect information about the network route and network distance between the scanner host and the target host.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Network route from scanner (10.0.0.116) to target (10.0.0.112):
10.0.0.116
10.0.0.112
Network distance between scanner and target: 2
```

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: `2022-10-17T11:13:19Z`

[return to 10.0.0.112]

2.1.11 Log 139/tcp

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary
This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
A SMB server is running on this port
```

Solution:

Log Method
Details: `SMB/CIFS Server Detection`
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: `2023-08-01T13:29:10Z`

[return to 10.0.0.112]

2.1.12 Log 80/tcp

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).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
It was possible to enumerate the following HTTP server banner(s):
Server banner                  | Enumeration technique
---------------------------------------------------------------------------
↪-----------------
Server: Apache/2.4.52 (Ubuntu) | Invalid HTTP 00.5 GET request (non-existent HTT
↪P version) to '/'
```

Solution:

Log Method
Details: `HTTP Server Banner Enumeration`
OID:1.3.6.1.4.1.25623.1.0.108708

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2025-01-31T15:39:24Z

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
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.

Quality of Detection (QoD): 80%

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪/#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.
```

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: Web Application Scanning Consolidation / Info Reporting

Summary

The script consolidates and reports various information for web application (formerly called '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 forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The Hostname/IP "10.0.0.112" 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.
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
This service seems to be able to host PHP scripts.
This service seems to be able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; Greenbone OS 22.04.27)" was used to ac
↪cess the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
http://10.0.0.112/
http://10.0.0.112/dvwa
http://10.0.0.112/mutillidae
http://10.0.0.112/mutillidae/src
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 web application scanning because th
↪e "Regex pattern to exclude directories from CGI scanning" setting of the VT "
↪Global variable 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|graph
↪ic|grafik|picture|bilder|thumbnail|media/|skins?/)"
http://10.0.0.112/icons
http://10.0.0.112/javascript
Directory index found at:
http://10.0.0.112/mutillidae/
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://10.0.0.112/mutillidae/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
```

Solution:

Log Method

Details: Web Application Scanning Consolidation / Info Reporting
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2024-09-19T05:05:57Z

References

url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: Check open ports

Summary

This plugin checks if the port scanners did not kill a service.

. . . continues on next page . . .

. . . continued from previous page . . .

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by a plugin
```

Solution:

Log Method

Details: `Check open ports`
OID:1.3.6.1.4.1.25623.1.0.10919
Version used: `2023-08-03T05:05:16Z`

Log (CVSS: 0.0)
NVT: Services

Summary

This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
A web server is running on this port
```

Solution:

Vulnerability Insight

This plugin attempts to guess which service is running on the remote port(s). 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.

Log Method

Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

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 . . .

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote HTTP Server banner is:
Server: Apache/2.4.52 (Ubuntu)
```

Solution:

Log Method

Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

[return to 10.0.0.112]

2.1.13 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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
10.0.0.112|cpe:/a:apache:http_server:2.4.52
10.0.0.112|cpe:/a:beasts:vsftpd:3.0.5
10.0.0.112|cpe:/a:isc:bind:9.18.30
10.0.0.112|cpe:/o:canonical:ubuntu_linux
```

Solution:

Log Method

Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `2022-07-27T10:11:28Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://nvd.nist.gov/products/cpe
```

[return to 10.0.0.112]

This file was automatically generated.