Scan Report

January 19, 2020

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 192.168.1.10". The scan started at Sun Jan 19 03:34:13 2020 UTC and ended at Sun Jan 19 03:55:18 2020 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
192.168.1.10 scanner	2	21	0	34	0
Total: 1	2	21	0	34	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.

This report contains all 57 results selected by the filtering described above. Before filtering there were 57 results.

2 Results per Host

2.1 192.168.1.10

Host scan start Sun Jan 19 03:34:24 2020 UTC
Host scan end Sun Jan 19 03:55:18 2020 UTC

Service (Port)	Threat Level
general/tcp	High
80/tcp	High
22/tcp	Medium
general/tcp	Medium
4000/tcp	Medium
2222/tcp	Medium
5901/tcp	Medium
80/tcp	Medium
23/tcp	Medium
6001/tcp	Log
22/tcp	Log
general/tcp	Log
4000/tcp	Log
2222/tcp	Log
general/CPE-T	Log
5901/tcp	Log
80/tcp	Log
23/tcp	Log

2.1.1 High general/tcp

High (CVSS: 7.2)
NVT: Apache HTTP Server < 2.4.39 Privilege Escalation Vulnerability (Linux)

Product detection result
cpe:/a:apache:http_server:2.4.29
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

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: 2.4.29
Fixed version: 2.4.39

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: 2019-04-15T07:08:44+0000

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.29
Method: Apache Web Server Detection
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
CVE: CVE-2019-0211
Other:
URL:https://httpd.apache.org/security/vulnerabilities_24.html

[return to 192.168.1.10]

2.1.2 High 80/tcp

High (CVSS: 7.8)
NVT: Apache HTTP Server Multiple Vulnerabilities (Linux)

Product detection result
`cpe:/a:apache:http_server:2.4.29`
`Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)`

Summary
Apache HTTP server is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 2.4.29`
`Fixed version: 2.4.41`

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

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server Multiple Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.114147
Version used: `2019-10-18T14:24:52+0000`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.29`
Method: `Apache Web Server Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
`CVE: CVE-2019-9517, CVE-2019-10081`
`Other:`
`URL:https://httpd.apache.org/security/vulnerabilities_24.html`

[return to 192.168.1.10]

2.1.3 Medium 22/tcp

Medium (CVSS: 5.0)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)

Product detection result
`cpe:/a:openbsd:openssh:7.6p1`
`Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)`

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
```
Installed version: 7.6p1
Fixed version:     None
Installation
path / port:       22/tcp
```

Impact
Successfully exploitation will allow remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

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

Affected Software/OS
OpenSSH version 5.9 to 7.8 on Linux.

Vulnerability Insight
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.813888
Version used: `2019-09-26T09:12:46+0000`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.6p1`

... continues on next page ...

... continued from previous page ...

Method: OpenSSH Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.108577)

References
CVE: CVE-2018-15919
Other:
URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163
URL:https://seclists.org/oss-sec/2018/q3/180

Medium (CVSS: 5.0)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result
cpe:/a:openbsd:openssh:7.6p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.6p1
Fixed version: 7.8
Installation
path / port: 22/tcp

Impact
Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution
Solution type: VendorFix
Update to version 7.8 or later.

Affected Software/OS
OpenSSH versions 7.7 and prior on Linux

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.813864
Version used: 2019-05-23T14:08:05+0000

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.6p1
Method: OpenSSH Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.108577)

References
CVE: CVE-2018-15473
Other:
URL:https://0day.city/cve-2018-15473.html
URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a
↪7d1e0

[return to 192.168.1.10]

2.1.4 Medium general/tcp

Medium (CVSS: 5.0)
NVT: Apache HTTP Server < 2.4.38 HTTP/2 DoS Vulnerability (Linux)

Product detection result
cpe:/a:apache:http_server:2.4.29
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

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

Vulnerability Detection Result
Installed version: 2.4.29
Fixed version: 2.4.38

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

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

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

... continues on next page ...

... continued from previous page ...

Details: Apache HTTP Server < 2.4.38 HTTP/2 DoS Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.141966
Version used: $Revision: 13547 $

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.29
Method: Apache Web Server Detection
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
CVE: CVE-2018-17189
Other:
URL:https://httpd.apache.org/security/vulnerabilities_24.html

Medium (CVSS: 5.0)
NVT: Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Linux)

Product detection result
cpe:/a:apache:http_server:2.4.29
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

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

Vulnerability Detection Result
Installed version: 2.4.29
Fixed version: 2.4.38

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.141964
Version used: $Revision: 13750 $

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:apache:http_server:2.4.29
Method: Apache Web Server Detection
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
CVE: CVE-2018-17199
Other:
URL:https://httpd.apache.org/security/vulnerabilities_24.html

Medium (CVSS: 6.0)
NVT: Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Linux)

Product detection result
cpe:/a:apache:http_server:2.4.29
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

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: 2.4.29
Fixed version: 2.4.39

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: 2019-04-15T07:08:44+0000

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.29
Method: Apache Web Server Detection
OID: 1.3.6.1.4.1.25623.1.0.900498)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2019-0217
Other:
URL:https://httpd.apache.org/security/vulnerabilities_24.html

Medium (CVSS: 5.0)
NVT: Apache HTTP Server < 2.4.39 mod_http2 DoS Vulnerability (Linux)

Product detection result
cpe:/a:apache:http_server:2.4.29
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

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: 2.4.29
Fixed version: 2.4.39

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server < 2.4.39 mod_http2 DoS Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.142226
Version used: 2019-04-08T15:50:06+0000

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.29
Method: Apache Web Server Detection
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
CVE: CVE-2019-0196
Other:
URL:https://httpd.apache.org/security/vulnerabilities_24.html

Medium (CVSS: 5.0)
NVT: Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Linux)

Product detection result
`cpe:/a:apache:http_server:2.4.29`
`Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)`

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

Vulnerability Detection Result
`Installed version: 2.4.29`
`Fixed version: 2.4.39`

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: `2019-06-17T06:50:08+0000`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.29`
Method: `Apache Web Server Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
`CVE: CVE-2019-0220`
`Other:`
`URL:https://httpd.apache.org/security/vulnerabilities_24.html`

[return to 192.168.1.10]

2.1.5 Medium 4000/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Solution
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

Affected Software/OS
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: $Revision: 5232 $

References
CVE: CVE-2016-2183, CVE-2016-6329
Other:
URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
URL:https://sweet32.info/

[return to 192.168.1.10]

2.1.6 Medium 2222/tcp

Medium (CVSS: 5.0)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:openbsd:openssh:7.6p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.6p1
Fixed version: None
Installation
path / port: 2222/tcp

Impact
Successfully exploitation will allow remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

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

Affected Software/OS
OpenSSH version 5.9 to 7.8 on Linux.

Vulnerability Insight
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.813888
Version used: 2019-09-26T09:12:46+0000

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.6p1
Method: OpenSSH Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.108577)

References
CVE: CVE-2018-15919
Other:

... continues on next page ...

... continued from previous page ...

URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163
URL:https://seclists.org/oss-sec/2018/q3/180

Medium (CVSS: 5.0)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)

Product detection result
cpe:/a:openbsd:openssh:7.6p1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.6p1
Fixed version: 7.8
Installation
path / port: 2222/tcp

Impact
Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution
Solution type: VendorFix
Update to version 7.8 or later.

Affected Software/OS
OpenSSH versions 7.7 and prior on Linux

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)
OID:1.3.6.1.4.1.25623.1.0.813864
Version used: 2019-05-23T14:08:05+0000

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.6p1
Method: OpenSSH Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.108577)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2018-15473
Other:
URL:https://0day.city/cve-2018-15473.html
URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d1e0

[return to 192.168.1.10]

2.1.7 Medium 5901/tcp

Medium (CVSS: 4.8)
NVT: VNC Server Unencrypted Data Transmission

Summary
The remote host is running a VNC server providing one or more insecure or cryptographically weak Security Type(s) not intended for use on untrusted networks.

Vulnerability Detection Result
The VNC server provides the following insecure or cryptographically weak Security Type(s):
2 (VNC authentication)

Impact
An attacker can uncover sensitive data by sniffing traffic to the VNC server.

Solution
Solution type: Mitigation
Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254]. Some VNC server vendors are also providing more secure Security Types within their products.

Vulnerability Detection Method
Details: VNC Server Unencrypted Data Transmission
OID:1.3.6.1.4.1.25623.1.0.108529
Version used: $Revision: 13014 $

References
Other:
URL:https://tools.ietf.org/html/rfc6143#page-10

[return to 192.168.1.10]

2.1.8 Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Apache /server-status accessible

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

Vulnerability Detection Result
`Vulnerable url: http://scanner/server-status`

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

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

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

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

Vulnerability Detection Method
Checks if the /server-status page of Apache is accessible.
Details: `Apache /server-status accessible`
OID:1.3.6.1.4.1.25623.1.0.10677
Version used: `2019-11-22T13:51:04+0000`

References
```
Other:
  URL:https://httpd.apache.org/docs/current/mod/mod_status.html
```

Medium (CVSS: 5.0)
NVT: Apache HTTP Server 'HTTP/2 connection' DoS Vulnerability

Product detection result
`cpe:/a:apache:http_server:2.4.29`
`Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)`

Summary
This host is running Apache HTTP Server and is prone to denial-of-service vulnerability

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
Installed version: 2.4.29
Fixed version: 2.4.34
Installation
path / port: 80/tcp

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

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

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server 'HTTP/2 connection' DoS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.813812
Version used: 2019-07-05T10:41:31+0000

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.29
Method: Apache Web Server Detection
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
CVE: CVE-2018-1333
Other:
URL:http://seclists.org/oss-sec/2018/q3/39
URL:https://httpd.apache.org/security/vulnerabilities_24.html

Medium (CVSS: 4.3)
NVT: Apache HTTP Server Denial of Service Vulnerability Apr18 (Linux)

Product detection result
cpe:/a:apache:http_server:2.4.29
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

... continues on next page ...

... continued from previous page ...

Summary
The host is installed with Apache HTTP server and is prone to a denial of service vulnerability.

Vulnerability Detection Result
Installed version: 2.4.29
Fixed version: 2.4.30
Installation
path / port: 80/tcp

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

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

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server Denial of Service Vulnerability Apr18 (Linux)
OID:1.3.6.1.4.1.25623.1.0.812845
Version used: 2019-05-03T08:55:39+0000

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.29
Method: Apache Web Server Detection
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
CVE: CVE-2018-1302
BID:103528
Other:
URL:https://httpd.apache.org/download.cgi
URL:http://www.openwall.com/lists/oss-security/2018/03/24/8
URL:http://www.openwall.com/lists/oss-security/2018/03/24/2

Medium (CVSS: 5.0)
NVT: Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Linux)

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:apache:http_server:2.4.29
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

Summary
The host is installed with Apache HTTP server and is prone to a denial of service vulnerability.

Vulnerability Detection Result
Installed version: 2.4.29
Fixed version: 2.4.30
Installation
path / port: 80/tcp

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

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

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Linux)
OID:1.3.6.1.4.1.25623.1.0.812849
Version used: 2019-05-03T08:55:39+0000

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.29
Method: Apache Web Server Detection
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
CVE: CVE-2018-1303
BID:103522
Other:
URL:https://httpd.apache.org/download.cgi

... continues on next page ...

... continued from previous page ...

URL:https://httpd.apache.org/security/vulnerabilities_24.html

Medium (CVSS: 6.4)
NVT: Apache HTTP Server Memory Access Vulnerability (Linux)

Product detection result
cpe:/a:apache:http_server:2.4.29
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

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

Vulnerability Detection Result
Installed version: 2.4.29
Fixed version: 2.4.41

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

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server Memory Access Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.114149
Version used: 2019-10-18T14:24:52+0000

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.29
Method: Apache Web Server Detection
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
CVE: CVE-2019-10082
Other:
URL:https://httpd.apache.org/security/vulnerabilities_24.html

Medium (CVSS: 5.8)
NVT: Apache HTTP Server Multiple Vulnerabilities (Linux)

Product detection result
`cpe:/a:apache:http_server:2.4.29`
`Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)`

Summary
Apache HTTP server is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 2.4.29`
`Fixed version: 2.4.41`

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

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server Multiple Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.114143
Version used: `2019-10-18T14:24:52+0000`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.29`
Method: `Apache Web Server Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
`CVE: CVE-2019-10092, CVE-2019-10098`
`Other:`
`URL:https://httpd.apache.org/security/vulnerabilities_24.html`

Medium (CVSS: 6.8)
NVT: Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux)

Product detection result
`cpe:/a:apache:http_server:2.4.29`
`Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)`

Summary
The host is installed with Apache HTTP server and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 2.4.29`
`Fixed version: 2.4.30`
`Installation path / port: 80/tcp`

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

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

Affected Software/OS
Apache HTTP server versions from 2.4.1 to 2.4.4, 2.4.6, 2.4.7, 2.4.9, 2.4.10, 2.4.12, 2.4.16 to 2.4.18, 2.4.20, 2.4.23, 2.4.25 to 2.4.29 on Linux.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.812844
Version used: `2019-05-03T08:55:39+0000`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.4.29`
Method: `Apache Web Server Detection`

. . . continues on next page . . .

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
CVE: CVE-2018-1312, CVE-2018-1283, CVE-2017-15715, CVE-2017-15710, CVE-2018-1301
BID:103524, 103520, 103525, 103512, 103515
Other:
  URL:https://httpd.apache.org/download.cgi
   URL:https://httpd.apache.org/security/vulnerabilities_24.html
```

Medium (CVSS: 4.3)
NVT: Apache HTTPD HTTP/2 'SETTINGS' Data Processing DoS Vulnerability (Linux)

Product detection result

```
cpe:/a:apache:http_server:2.4.29
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
```

Summary

This host is running Apache HTTP Server and is prone to denial-of-service vulnerability

Vulnerability Detection Result

```
Installed version: 2.4.29
Fixed version:     2.4.35
Installation
path / port:       80/tcp
```

Impact

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

Solution

Solution type: VendorFix

Upgrade to Apache HTTP Server 2.4.35 or later. Please see the references for more information.

Affected Software/OS

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

Vulnerability Insight

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

Vulnerability Detection Method

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

Details: `Apache HTTPD HTTP/2 'SETTINGS' Data Processing DoS Vulnerability (Linux)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.814056
Version used: 2019-07-05T10:41:31+0000

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.29
Method: Apache Web Server Detection
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
CVE: CVE-2018-11763
Other:
URL:https://securitytracker.com/id/1041713
URL:https://httpd.apache.org/security/vulnerabilities_24.html

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 URLs requires Basic Authentication (URL:realm name):
http://scanner/:"Restricted Content"

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'

... continues on next page ...

... continued from previous page ...

Details: Cleartext Transmission of Sensitive Information via HTTP
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: $Revision: 10726 $

References
Other:
URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_S
↪ession_Management
URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
URL:https://cwe.mitre.org/data/definitions/319.html

[return to 192.168.1.10]

2.1.9 Medium 23/tcp

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

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

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

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

Solution
Solution type: Mitigation
Replace Telnet with a protocol like SSH which supports encrypted connections.

Vulnerability Detection Method
Details: Telnet Unencrypted Cleartext Login
OID:1.3.6.1.4.1.25623.1.0.108522
Version used: 2019-06-06T07:39:31+0000

[return to 192.168.1.10]

2.1.10 Log 6001/tcp

Log (CVSS: 0.0)
NVT: X Server Detection

... continues on next page ...

... continued from previous page ...

Summary
This plugin detects X Window servers.
X11 is a client - server protocol. Basically, the server is in charge of the screen, and the clients connect to it and send several requests like drawing a window or a menu, and the server sends events back to the clients, such as mouse clicks, key strokes, and so on...
An improperly configured X server will accept connections from clients from anywhere. This allows an attacker to make a client connect to the X server to record the keystrokes of the user, which may contain sensitive information, such as account passwords. This can be prevented by using xauth, MIT cookies, or preventing the X server from listening on TCP (a Unix sock is used for local connections)

Vulnerability Detection Result
```
Detected X Windows Server
Version:       11.0
Location:      6001/tcp
CPE:           cpe:/a:x.org:x11:11.0
Concluded from version/product identification result:
11.0
Extra information:
Server answered with: No protocol specified
```

Log Method
Details: `X Server Detection`
OID:1.3.6.1.4.1.25623.1.0.10407
Version used: `$Revision: 10123 $`

[return to 192.168.1.10]

2.1.11 Log 22/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
```
An ssh server is running on this port
```

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2019-07-08T14:12:44+0000`

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported

Summary
This script detects which algorithms are supported by the remote SSH Service.

Vulnerability Detection Result

```
The following options are supported by the remote ssh service:
kex_algorithms:
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nist
↪p384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-gr
↪oup16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffi
↪e-hellman-group14-sha1
server_host_key_algorithms:
ssh-rsa,rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519
encryption_algorithms_client_to_server:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
encryption_algorithms_server_to_client:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
mac_algorithms_client_to_server:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
mac_algorithms_server_to_client:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
compression_algorithms_client_to_server:
none,zlib@openssh.com
compression_algorithms_server_to_client:
none,zlib@openssh.com
```

Log Method
Details: `SSH Protocol Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: `2019-10-28T15:06:41+0000`

Log (CVSS: 0.0)
NVT: SSH Protocol Versions Supported

Summary
Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result

```
The remote SSH Server supports the following SSH Protocol Versions:
2.0
SSHv2 Fingerprint(s):
ecdsa-sha2-nistp256: 17:a8:54:6e:2f:99:84:68:58:fc:da:8a:0c:e3:cf:c7
ssh-ed25519: 9b:c0:8d:87:8e:c4:bf:8e:32:7e:79:83:fb:e7:e8:2f
ssh-rsa: c1:c6:1f:37:e1:67:26:74:7a:b2:ab:d5:21:49:10:66
```

Log Method

Details: `SSH Protocol Versions Supported`
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: `$Revision: 13594 $`

Log (CVSS: 0.0)
NVT: SSH Server type and version

Summary

This detects the SSH Server's type and version by connecting to the server and processing the buffer received.
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Vulnerability Detection Result

```
Remote SSH server banner: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
Remote SSH supported authentication: password,publickey
Remote SSH text/login banner: (not available)
This is probably:
- OpenSSH
Concluded from remote connection attempt with credentials:
Login:    OpenVAS-VT
Password: OpenVAS-VT
```

Log Method

Details: `SSH Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: `2019-10-30T07:03:08+0000`

[return to 192.168.1.10]

2.1.12 Log general/tcp

Log (CVSS: 0.0)
NVT: OpenSSH Detection Consolidation

Summary

... continues on next page ...

... continued from previous page ...

The script reports a detected OpenSSH including the version number.

Vulnerability Detection Result

```
Detected OpenSSH Server
Version:       7.6p1
Location:      22/tcp
CPE:           cpe:/a:openbsd:openssh:7.6p1
Concluded from version/product identification result:
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
Detected OpenSSH Server
Version:       7.6p1
Location:      2222/tcp
CPE:           cpe:/a:openbsd:openssh:7.6p1
Concluded from version/product identification result:
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
```

Log Method

Details: `OpenSSH Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.108577
Version used: `2019-05-23T06:42:35+0000`

References

```
Other:
  URL:https://www.openssh.com/
```

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

Summary

This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

Vulnerability Detection Result

```
Best matching OS:
OS:            Ubuntu
Version:       18.04
CPE:           cpe:/o:canonical:ubuntu_linux:18.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification)
Concluded from SSH banner on port 2222/tcp: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu
↪0.3
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS:            Ubuntu
```

... continues on next page ...

... continued from previous page ...

```
Version:      18.04
CPE:          cpe:/o:canonical:ubuntu_linux:18.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification)
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.
↪3
OS:           Ubuntu
Version:      18.04
CPE:          cpe:/o:canonical:ubuntu_linux:18.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.4.29 (Ubuntu)
OS:           Ubuntu
CPE:          cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111069 (Telnet OS Identification)
Concluded from Telnet banner on port 23/tcp: Ubuntu 18.04.3 LTS
scanner login:
```

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2020-01-10T06:09:19+0000

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: SSL/TLS: Hostname discovery from server certificate

Summary
It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.

Vulnerability Detection Result

```
The following additional but not resolvable hostnames were detected:
test
```

Log Method
Details: SSL/TLS: Hostname discovery from server certificate
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: $Revision: 13774 $

Log (CVSS: 0.0)
NVT: Traceroute

Summary

... continues on next page ...

... continued from previous page ...

A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result

```
Here is the route from 192.168.1.10 to 192.168.1.10:
192.168.1.10
```

Solution

Block unwanted packets from escaping your network.

Log Method

Details: `Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `2019-09-09T06:03:58+0000`

[return to 192.168.1.10]

2.1.13 Log 4000/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary

The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result

```
The Hostname/IP "scanner" 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.
This service is marked as broken and no CGI scanning is launched against it. Rea
↪son:
-----
The remote web server is very slow - it took 99 seconds (Maximum response time c
```

... continues on next page ...

... continued from previous page ...

```
↪onfigured in 'Response Time / No 404 Error Code Check' (OID: 1.3.6.1.4.1.25623
↪.1.0.10386) preferences: 60 seconds) to execute the plugin no404.nasl (it usua
↪lly only takes a few seconds).
In order to keep the scan total time to a reasonable amount, the remote web serv
↪er has not been tested.
If the remote server should be tested it has to be fixed to have it reply to the
↪ scanners requests in a reasonable amount of time. Alternatively the 'Maximum
↪response time (in seconds)' preference could be raised to a higher value if lo
↪nger scan times are accepted.
-----
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access
↪the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
https://scanner:4000/
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
```

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2019-09-23T09:25:24+0000

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: Response Time / No 404 Error Code Check

Summary
This VT tests if the remote web server does not reply with a 404 error code and checks if it is replying to the scanners requests in a reasonable amount of time.

Vulnerability Detection Result

```
The remote web server is very slow - it took 99 seconds (Maximum response time c
↪onfigured in 'Response Time / No 404 Error Code Check' (OID: 1.3.6.1.4.1.25623
↪.1.0.10386) preferences: 60 seconds) to execute the plugin no404.nasl (it usua
↪lly only takes a few seconds).
In order to keep the scan total time to a reasonable amount, the remote web serv
```

... continues on next page ...

... continued from previous page ...

```
↪er has not been tested.
If the remote server should be tested it has to be fixed to have it reply to the
↪ scanners requests in a reasonable amount of time. Alternatively the 'Maximum
↪response time (in seconds)' preference could be raised to a higher value if lo
↪nger scan times are accepted.
```

Vulnerability Insight
This web server might show the following issues:
- it is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page or authentication page instead.
The Scanner might enabled some counter measures for that, however they might be insufficient.
If a great number of security issues are reported for this port, they might not all be accurate.
- it doesn't response in a reasonable amount of time to various HTTP requests sent by this VT.
In order to keep the scan total time to a reasonable amount, the remote web server might not be tested. If the remote server should be tested it has to be fixed to have it reply to the scanners requests in a reasonable amount of time.
Alternatively the 'Maximum response time (in seconds)' preference could be raised to a higher value if longer scan times are accepted.

Log Method
Details: `Response Time / No 404 Error Code Check`
OID:1.3.6.1.4.1.25623.1.0.10386
Version used: `2019-11-12T09:49:27+0000`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A TLScustom server answered on this port`

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2019-07-08T14:12:44+0000`

Log (CVSS: 0.0)
NVT: Services

Summary

... continues on next page ...

... continued from previous page ...

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
A web server is running on this port through SSL

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2019-07-08T14:12:44+0000

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Vulnerability Detection Result
```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "scanner".
Certificate details:
subject ...: C=DE,L=Osnabrueck,O=OpenVAS Users,CN=test
subject alternative names (SAN):
None
issued by .: C=DE,L=Osnabrueck,O=OpenVAS Users,OU=Certificate Authority for test
serial ....: 5E20B3911CAE386EAE5E0EBF
valid from : 2020-01-16 19:03:45 UTC
valid until: 2022-01-15 19:03:45 UTC
fingerprint (SHA-1): 064A73C6DEB66A9EFA504F02464701B7DCBAC5F0
fingerprint (SHA-256): 40EE013D607BA2C33D2E793F5FE3FD5A8F1FE7A16D57BF4E73395E8B9
↪78E9275
```

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: $Revision: 8981 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
subject ...: C=DE,L=Osnabrueck,O=OpenVAS Users,CN=test
subject alternative names (SAN):
None
issued by .: C=DE,L=Osnabrueck,O=OpenVAS Users,OU=Certificate Authority for test
serial ....: 5E20B3911CAE386EAE5E0EBF
valid from : 2020-01-16 19:03:45 UTC
valid until: 2022-01-15 19:03:45 UTC
fingerprint (SHA-1): 064A73C6DEB66A9EFA504F02464701B7DCBAC5F0
fingerprint (SHA-256): 40EE013D607BA2C33D2E793F5FE3FD5A8F1FE7A16D57BF4E73395E8B9
↪78E9275
```

Log Method

Details: `SSL/TLS: Collect and Report Certificate Details`
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: `2019-04-04T13:38:03+0000`

Log (CVSS: 0.0)
NVT: SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing

Summary

The remote service is missing support for SSL/TLS cipher suites supporting Perfect Forward Secrecy.

Vulnerability Detection Result

```
The remote service does not support perfect forward secrecy cipher suites.
```

Log Method

Details: `SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing`
OID:1.3.6.1.4.1.25623.1.0.105092
Version used: `$Revision: 4736 $`

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Medium Cipher Suites

Summary

This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result

```
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
```

... continues on next page ...

... continued from previous page ...

```
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384
```

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium

Log Method
Details: `SSL/TLS: Report Medium Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: `$Revision: 4743 $`

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Non Weak Cipher Suites

Summary
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result

```
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
```

... continues on next page ...

... continued from previous page ...

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: $Revision: 4736 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Supported Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service.
As the NVT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result
No 'Strong' cipher suites accepted by this service via the TLSv1.0 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
No 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Strong' cipher suites accepted by this service via the TLSv1.1 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

... continues on next page ...

... continued from previous page ...

```
No 'Weak' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384
No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.
```

Log Method
Details: SSL/TLS: Report Supported Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: $Revision: 11108 $

[return to 192.168.1.10]

2.1.14 Log 2222/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
An ssh server is running on this port

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2019-07-08T14:12:44+0000

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported

Summary
This script detects which algorithms are supported by the remote SSH Service.

Vulnerability Detection Result

```
The following options are supported by the remote ssh service:
kex_algorithms:
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nist
↪p384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-gr
↪oup16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffi
↪e-hellman-group14-sha1
server_host_key_algorithms:
ssh-rsa,rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519
encryption_algorithms_client_to_server:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
encryption_algorithms_server_to_client:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
mac_algorithms_client_to_server:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
mac_algorithms_server_to_client:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
compression_algorithms_client_to_server:
none,zlib@openssh.com
compression_algorithms_server_to_client:
none,zlib@openssh.com
```

Log Method
Details: `SSH Protocol Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: `2019-10-28T15:06:41+0000`

Log (CVSS: 0.0)
NVT: SSH Protocol Versions Supported

Summary
Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result

```
The remote SSH Server supports the following SSH Protocol Versions:
2.0
SSHv2 Fingerprint(s):
ecdsa-sha2-nistp256: 17:a8:54:6e:2f:99:84:68:58:fc:da:8a:0c:e3:cf:c7
ssh-ed25519: 9b:c0:8d:87:8e:c4:bf:8e:32:7e:79:83:fb:e7:e8:2f
ssh-rsa: c1:c6:1f:37:e1:67:26:74:7a:b2:ab:d5:21:49:10:66
```

Log Method

Details: `SSH Protocol Versions Supported`
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: `$Revision: 13594 $`

Log (CVSS: 0.0)
NVT: SSH Server type and version

Summary

This detects the SSH Server's type and version by connecting to the server and processing the buffer received.
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Vulnerability Detection Result

```
Remote SSH server banner: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
Remote SSH supported authentication: password,publickey
Remote SSH text/login banner: (not available)
This is probably:
- OpenSSH
Concluded from remote connection attempt with credentials:
Login:    OpenVAS-VT
Password: OpenVAS-VT
```

Log Method

Details: `SSH Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: `2019-10-30T07:03:08+0000`

[return to 192.168.1.10]

2.1.15 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary

... continues on next page ...

... continued from previous page ...

This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.
Note: Some CPEs for specific products might show up twice or more in the output. Background: After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.

Vulnerability Detection Result
192.168.1.10|cpe:/a:apache:http_server:2.4.29
192.168.1.10|cpe:/a:openbsd:openssh:7.6p1
192.168.1.10|cpe:/a:x.org:x11:11.0
192.168.1.10|cpe:/o:canonical:ubuntu_linux:18.04

Log Method
Details: CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: 2019-10-24T11:29:24+0000

References
Other:
URL:https://nvd.nist.gov/products/cpe

[return to 192.168.1.10]

2.1.16 Log 5901/tcp

Log (CVSS: 9.0)
NVT: VNC Brute Force Login

Summary
Try to log in with given passwords via VNC protocol.

Vulnerability Detection Result
Too many unsuccessful connection attempts are made which means the scanner IP go
↪t blocked. Therefore the brute force check was aborted.

Solution
Solution type: Mitigation
Change the password to something hard to guess or enable password protection at all.

Vulnerability Insight
This script tries to authenticate to a VNC server with the passwords set in the password preference. It will also test and report if no authentication / password is required at all.
Note: Some VNC servers have a blacklisting scheme that blocks IP addresses after five unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked.

... continues on next page ...

... continued from previous page ...

Note as well that passwords can be max. 8 characters long.

Vulnerability Detection Method
Details: `VNC Brute Force Login`
OID:1.3.6.1.4.1.25623.1.0.106056
Version used: `2019-12-03T12:31:12+0000`

Log (CVSS: 0.0)
NVT: VNC security types

Summary
This script checks the remote VNC protocol version and the available 'security types'.

Vulnerability Detection Result
```
The remote VNC server supports those security types:
2 (VNC authentication)
```

Log Method
Details: `VNC security types`
OID:1.3.6.1.4.1.25623.1.0.19288
Version used: `$Revision: 13541 $`

Log (CVSS: 0.0)
NVT: VNC Server and Protocol Version Detection

Summary
The remote host is running a remote display software (VNC) which permits a console to be displayed remotely.
This allows authenticated users of the remote host to take its control remotely.

Vulnerability Detection Result
```
A VNC server seems to be running on this port.
The version of the VNC protocol is : RFB 003.008
```

Solution
Make sure the use of this software is done in accordance with your corporate security policy, filter incoming traffic to this port.

Log Method
Details: `VNC Server and Protocol Version Detection`
OID:1.3.6.1.4.1.25623.1.0.10342
Version used: `$Revision: 13541 $`

[return to 192.168.1.10]

2.1.17 Log 80/tcp

Log (CVSS: 0.0)
NVT: Apache Web Server Detection

Summary
Detects the installed version of Apache Web Server
The script detects the version of Apache HTTP Server on remote host and sets the KB.

Vulnerability Detection Result
```
Detected Apache
Version:       2.4.29
Location:      80/tcp
CPE:           cpe:/a:apache:http_server:2.4.29
Concluded from version/product identification result:
Server: Apache/2.4.29
```

Log Method
Details: `Apache Web Server Detection`
OID:1.3.6.1.4.1.25623.1.0.900498
Version used: `2019-11-12T09:49:27+0000`

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result
```
The Hostname/IP "scanner" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access
```

... continues on next page ...

... continued from previous page ...

```
↪the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories require authentication and are tested by the script "H
↪TTP Brute Force Logins with default Credentials (OID: 1.3.6.1.4.1.25623.1.0.10
↪8041)":
http://scanner/
The following directories were used for CGI scanning:
http://scanner/
http://scanner/server-status
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
The following directories were excluded from CGI scanning because the "Regex pat
↪tern to exclude directories from CGI scanning" setting of the NVT "Global vari
↪able settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\
↪.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|p
↪icture|bilder|thumbnail|media/|skins?/)"
http://scanner/icons
```

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2019-09-23T09:25:24+0000

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This detects the HTTP Server's type and version.

Vulnerability Detection Result
The remote web server type is :
Apache/2.4.29 (Ubuntu)
Solution : You can set the directive "ServerTokens Prod" to limit
the information emanating from the server in its response headers.

Solution
- Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display'
- Be sure to remove common logos like apache_pb.gif.

... continues on next page ...

... continued from previous page ...

- With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2019-12-17T11:41:26+0000`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A web server is running on this port`

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2019-07-08T14:12:44+0000`

[return to 192.168.1.10]

2.1.18 Log 23/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A telnet server seems to be running on this port`

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2019-07-08T14:12:44+0000`

Log (CVSS: 0.0)
NVT: Telnet Banner Reporting

Summary
This scripts reports the received banner of a Telnet service.

Vulnerability Detection Result
```
Remote Telnet banner:
Ubuntu 18.04.3 LTS
scanner login:
```

Log Method
Details: `Telnet Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.10281
Version used: `2019-12-17T07:47:12+0000`

Log (CVSS: 0.0)
NVT: Telnet Service Detection

Summary
This scripts tries to detect a Telnet service running at the remote host.

Vulnerability Detection Result
```
A Telnet server seems to be running on this port
```

Log Method
Details: `Telnet Service Detection`
OID:1.3.6.1.4.1.25623.1.0.100074
Version used: `$Revision: 13541 $`

References
```
Other:
  URL:https://tools.ietf.org/html/rfc854
```

[return to 192.168.1.10]