Scan Report

March 6, 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 "Network scan". The scan started at Thu Mar 6 02:13:53 2025 UTC and ended at Thu Mar 6 06:45:28 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**
2.1 192.168.2.108 . . . 2
2.1.1 High 443/tcp . . . 3
2.1.2 Log general/tcp . . . 3
2.1.3 Log 80/tcp . . . 7
2.1.4 Log 443/tcp . . . 10
2.1.5 Log general/CPE-T . . . 28
2.2 192.168.2.1 . . . 29
2.2.1 High 443/tcp . . . 29
2.2.2 High 80/tcp . . . 33
2.2.3 Medium 9443/tcp . . . 33
2.2.4 Medium 443/tcp . . . 38
2.2.5 Medium 80/tcp . . . 56
2.2.6 Low general/icmp . . . 71
2.2.7 Log general/CPE-T . . . 72
2.2.8 Log 445/tcp . . . 73
2.2.9 Log 53/tcp . . . 75
2.2.10 Log general/tcp . . . 76
2.2.11 Log 9443/tcp . . . 81

2.2.12 Log 443/tcp . . . 84
2.2.13 Log 10080/tcp . . . 102
2.2.14 Log 80/tcp . . . 107
2.2.15 Log 9000/tcp . . . 114
2.3 192.168.2.66 . . . 119
2.3.1 Medium 443/tcp . . . 119
2.3.2 Low general/icmp . . . 120
2.3.3 Low general/tcp . . . 121
2.3.4 Log 2020/tcp . . . 122
2.3.5 Log 443/tcp . . . 123
2.3.6 Log 8800/tcp . . . 136
2.3.7 Log general/CPE-T . . . 139
2.3.8 Log 554/tcp . . . 140
2.3.9 Log 10443/tcp . . . 141
2.3.10 Log general/tcp . . . 146
2.4 192.168.2.107 . . . 149
2.4.1 Low general/tcp . . . 149
2.4.2 Low general/icmp . . . 150
2.4.3 Log general/CPE-T . . . 151
2.4.4 Log 9200/tcp . . . 152
2.4.5 Log general/tcp . . . 156
2.5 192.168.2.98 . . . 159
2.5.1 Low general/tcp . . . 159
2.5.2 Log general/tcp . . . 160
2.5.3 Log 7680/tcp . . . 162
2.6 192.168.2.106 . . . 163
2.6.1 Low general/icmp . . . 163
2.6.2 Low general/tcp . . . 164
2.6.3 Log general/tcp . . . 165
2.6.4 Log 443/tcp . . . 170
2.6.5 Log 80/tcp . . . 188
2.6.6 Log general/CPE-T . . . 191
2.7 192.168.2.105 . . . 192
2.7.1 Low general/icmp . . . 192
2.7.2 Log general/tcp . . . 193
2.7.3 Log general/CPE-T . . . 195
2.8 192.168.2.61 . . . 196
2.8.1 Low general/icmp . . . 196
2.8.2 Log general/tcp . . . 197
2.8.3 Log general/CPE-T . . . 200

2.9 192.168.2.88 200
2.9.1 Log general/tcp 200
2.9.2 Log general/CPE-T 202
2.10 192.168.2.20 203
2.10.1 Log general/tcp 203

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.2.108	1	0	0	32	0
192.168.2.1 mynetwork.home	3	20	1	59	0
192.168.2.66	0	1	2	35	0
192.168.2.107	0	0	2	9	0
192.168.2.98	0	0	1	4	0
192.168.2.106	0	0	2	33	0
192.168.2.105	0	0	1	5	0
192.168.2.61	0	0	1	5	0
192.168.2.88	0	0	0	4	0
192.168.2.20	0	0	0	3	0
Total: 10	4	21	10	189	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 224 results selected by the filtering described above. Before filtering there were 224 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.2.1 - mynetwork.home	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 192.168.2.108

Host scan start	Thu Mar 6 02:25:27 2025 UTC
Host scan end	Thu Mar 6 04:55:40 2025 UTC

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

2.1.1 High 443/tcp

High (CVSS: 10.0)
NVT: Greenbone Security Assistant (GSA) Default Credentials (HTTP)

Summary
The remote Greenbone Security Assistant (GSA) is installed / configured in a way that it has account(s) with default passwords enabled.

Quality of Detection (QoD): 100%

Vulnerability Detection Result
`It was possible to login using the following credentials (username:password): admin:admin`

Impact
This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.

Solution:
Solution type: Workaround
Change the password of the mentioned account(s).

Vulnerability Detection Method
Tries to login with known default credentials via the HTTP protocol.
Details: `Greenbone Security Assistant (GSA) Default Credentials (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.105354
Version used: `2024-07-10T05:05:27Z`

[return to 192.168.2.108]

2.1.2 Log general/tcp

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

Summary

. . . continues on next page . . .

... continued from previous page ...

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:           Greenbone OS (GOS) 22.04.27
Version:      22.04.27
CPE:          cpe:/o:greenbone:greenbone_os:22.04.27
Found by VT:  1.3.6.1.4.1.25623.1.0.103220 (Greenbone Security Manager (GSM) / G
↪reenbone OS (GOS) Detection Consolidation)
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:  1.3.6.1.4.1.25623.1.0.103841 (Greenbone Security Assistant (GSA) D
↪etection (HTTP))
```

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: nginx Detection Consolidation

Summary
Consolidation of nginx detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected nginx
Version:       unknown
Location:      443/tcp
```

... continues on next page ...

... continued from previous page ...

```
CPE:           cpe:/a:nginx:nginx
Concluded from version/product identification result:
Server: nginx
Detected nginx
Version:       unknown
Location:      80/tcp
CPE:           cpe:/a:nginx:nginx
Concluded from version/product identification result:
Server: nginx
<hr><center>nginx</center>
Concluded from version/product identification location:
http://192.168.2.108/
```

Solution:

Log Method
Details: `nginx Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.113787
Version used: `2022-02-03T09:26:44Z`

References
`url: https://www.nginx.com/`

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 (192.168.2.108) to target (192.168.2.108):
192.168.2.108
Network distance between scanner and target: 1
```

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

... continues on next page ...

... continued from previous page ...

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

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 192.168.2.108:
Hostname|Source
192.168.2.108|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: 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.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
```
The following additional and resolvable hostnames pointing to a different host i
↪p were detected:
gsm.gbuser.net
```

Solution:

Log Method

... continues on next page ...

... continued from previous page ...

Details: SSL/TLS: Hostname discovery from server certificate
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: 2021-11-22T15:32:39Z

Log (CVSS: 0.0)
NVT: Greenbone Security Manager (GSM) / Greenbone OS (GOS) Detection Consolidation

Summary
Consolidation of Greenbone Security Manager (GSM) / Greenbone OS (GOS) detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected Greenbone OS (GOS)
Version:        22.04.27
Location:       /
CPE:            cpe:/o:greenbone:greenbone_os:22.04.27
Detected Greenbone Security Manager (GSM) TRIAL
Location:       /
CPE:            cpe:/a:greenbone:gsm_trial
Detection methods:
- HTTP(s) on port 443/tcp
  Concluded from version/product identification result: vendorVersion: 'Greenbon
↪e OS 22.04.27',<newline>vendorLabel: 'gsm-trial_label.svg',
  Concluded from version/product identification location: https://192.168.2.108/
↪login and https://192.168.2.108/config.js
```

Solution:

Log Method
Details: Greenbone Security Manager (GSM) / Greenbone OS (GOS) Detection Consolidation
OID:1.3.6.1.4.1.25623.1.0.103220
Version used: 2022-08-11T10:10:35Z

[return to 192.168.2.108]

2.1.3 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).

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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

Solution:

Log Method

Details: `HTTP Server Banner Enumeration`
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: `2025-01-31T15:39:24Z`

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 "192.168.2.108" 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 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
```

... continues on next page ...

... continued from previous page ...

```
↪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://192.168.2.108/
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
```

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: 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: 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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The host returns a 30x (e.g. 301) error code when a non-existent file is request ↪ed. Some HTTP-related checks have been disabled.`

Solution:

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, authentication page or redirect 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: `2023-07-07T05:05:26Z`

[return to 192.168.2.108]

2.1.4 Log 443/tcp

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection

Product detection result
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25 ↪623.1.0.103692)`

... continues on next page ...

... continued from previous page ...

Summary
The SSL/TLS certificate on this port is self-signed.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
The certificate of the remote service is self signed.
Certificate details:
fingerprint (SHA-1)             | D3C255C6D78958DDE7DAD760D290E990E4C02A08
fingerprint (SHA-256)           | 2033B1DCFC10EC3189B15C5E6CE7791BB257D53783A03B
↪55CBD9C612393B4860
issued by                       | C=DE,ST=Niedersachsen,L=Osnabrueck,O=Greenbone
↪ AG Customer,OU=Vulnerability Management Team,CN=gsm.gbuser.net
public key algorithm            | RSA
public key size (bits)          | 3072
serial                          | 0CC5B263F56BB28519DD46EB06981D5225624BD1
signature algorithm             | sha256WithRSAEncryption
subject                         | C=DE,ST=Niedersachsen,L=Osnabrueck,O=Greenbone
↪ AG Customer,OU=Vulnerability Management Team,CN=gsm.gbuser.net
subject alternative names (SAN) | gsm.gbuser.net
valid from                      | 2025-02-07 07:40:09 UTC
valid until                     | 2027-02-07 07:40:09 UTC
```

Solution:

Log Method
Details: SSL/TLS: Certificate - Self-Signed Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

References
url: http://en.wikipedia.org/wiki/Self-signed_certificate

Log (CVSS: 0.0)
NVT: robot.txt / robots.txt exists on the Web Server (HTTP)

Summary

... continues on next page ...

... continued from previous page ...

Web Servers can use a file called /robot(s).txt to ask search engines to ignore certain files and directories. By nature this file can not be used to protect private files from public read access.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The file 'https://192.168.2.108/robots.txt' contains the following:
User-agent: *
Disallow: /
```

Solution:
Solution type: Mitigation
Review the content of the /robot(s).txt file and consider removing the files from the server or protect them in other ways in case you actually intended non-public availability.

Vulnerability Insight
Any serious web search engine will honor the /robot(s).txt file and not scan the files and directories listed there.
Any entries listed in this file are not even hidden anymore.

Log Method
Details: `robot.txt / robots.txt exists on the Web Server (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.10302
Version used: `2024-02-26T14:36:40Z`

References
`url: https://www.robotstxt.org/`
`url: https://www.robotstxt.org/norobots-rfc.txt`

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing

Summary
The remote web server is not enforcing HTTP Strict Transport Security (HSTS).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote web server is not enforcing HSTS.
HTTP-Banner:
HTTP/1.1 200 OK
Server: nginx
Date: ***replaced***
Content-Type: text/html; charset=utf-8
Content-Length: ***replaced***
```

... continues on next page ...

... continued from previous page ...

```
Connection: close
Last-Modified: ***replaced***
Expires: ***replaced***
Expires: ***replaced***
Cache-Control: no-cache, no-store
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'none'; object-src 'none'; base-uri 'none';
↪ connect-src 'self'; script-src 'self'; script-src-elem 'self' 'unsafe-inline'
↪;frame-ancestors 'none'; form-action 'self'; style-src-elem 'self' 'unsafe-inl
↪ine'; style-src 'self' 'unsafe-inline'; font-src 'self';img-src 'self' blob:;
Access-Control-Allow-Origin: gsm.gbuser.net
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
```

Solution:
Solution type: Workaround
Enable HSTS or add / configure the required directives correctly following the guides linked in the references.
Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code.
- Apache: Use 'Header always set' instead of 'Header set'.
- nginx: Append the 'always' keyword to each 'add_header' directive.
For different applications or web severs please refer to the related documentation for a similar configuration possibility.

Log Method
Details: `SSL/TLS: HTTP Strict Transport Security (HSTS) Missing`
OID:1.3.6.1.4.1.25623.1.0.105879
Version used: `2024-02-08T05:05:59Z`

References

```
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transpor
↪t_Security_Cheat_Sheet.html
url: https://owasp.org/www-project-secure-headers/#http-strict-transport-securit
↪y-hsts
url: https://tools.ietf.org/html/rfc6797
url: https://securityheaders.io/
url: https://httpd.apache.org/docs/current/mod/mod_headers.html#header
url: https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header
```

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing

Summary
The remote web server is not enforcing HTTP Public Key Pinning (HPKP).
Note: Most major browsers have dropped / deprecated support for this header in 2020.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote web server is not enforcing HPKP.
HTTP-Banner:
HTTP/1.1 200 OK
Server: nginx
Date: ***replaced***
Content-Type: text/html; charset=utf-8
Content-Length: ***replaced***
Connection: close
Last-Modified: ***replaced***
Expires: ***replaced***
Expires: ***replaced***
Cache-Control: no-cache, no-store
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'none'; object-src 'none'; base-uri 'none';
↪ connect-src 'self'; script-src 'self'; script-src-elem 'self' 'unsafe-inline'
↪;frame-ancestors 'none'; form-action 'self'; style-src-elem 'self' 'unsafe-inl
↪ine'; style-src 'self' 'unsafe-inline'; font-src 'self';img-src 'self' blob:;
Access-Control-Allow-Origin: gsm.gbuser.net
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
```

Solution:
Solution type: Workaround
Enable HPKP or add / configure the required directives correctly following the guides linked in the references.
Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code.
- Apache: Use 'Header always set' instead of 'Header set'.
- nginx: Append the 'always' keyword to each 'add_header' directive.
For different applications or web severs please refer to the related documentation for a similar configuration possibility.

... continues on next page ...

... continued from previous page ...

Log Method
Details: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing
OID:1.3.6.1.4.1.25623.1.0.108247
Version used: 2024-02-08T05:05:59Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-for-http-hpkp
url: https://tools.ietf.org/html/rfc7469
url: https://securityheaders.io/
url: https://httpd.apache.org/docs/current/mod/mod_headers.html#header
url: https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

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

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)

Summary
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Quality of Detection (QoD): 98%

Vulnerability Detection Result
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

Solution:

Log Method
Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: 2024-09-30T08:38:05Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security

... continues on next page ...

... continued from previous page ...

Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

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

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

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256

Solution:

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: 2024-09-27T05:05:23Z

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

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

Product detection result

... continues on next page ...

... continued from previous page ...

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

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
'Non Weak' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

Solution:

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: 2024-09-27T05:05:23Z

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

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

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
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_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256

... continues on next page ...

... continued from previous page ...

```
TLS_RSA_WITH_AES_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.
'Strong' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
No 'Weak' cipher suites accepted by this service via the TLSv1.3 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.3 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.3 protocol.
```

Solution:

Vulnerability Insight
Notes:
- As the VT '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 VT instead.
- SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Log Method
Details: SSL/TLS: Report Supported Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Safe/Secure Renegotiation Support Status

Summary
Checks and reports if a remote SSL/TLS service supports safe/secure renegotiation.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
Protocol Version | Safe/Secure Renegotiation Support Status
------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪-----------------------------------
SSLv3            | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.0          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
```

... continues on next page ...

... continued from previous page ...

```
↪pting this SSL/TLS protocol version).
TLSv1.1          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.2          | Enabled, Note: While the remote service announces the support
↪ of safe/secure renegotiation it still might not support / accept renegotiatio
↪n at all.
TLSv1.3          | Disabled (The TLSv1.3 protocol generally doesn't support rene
↪gotiation so this is always reported as 'Disabled')
```

Solution:

Log Method
Details: SSL/TLS: Safe/Secure Renegotiation Support Status
OID:1.3.6.1.4.1.25623.1.0.117757
Version used: 2024-09-27T05:05:23Z

References
url: https://www.gnutls.org/manual/html_node/Safe-renegotiation.html
url: https://wiki.openssl.org/index.php/TLS1.3#Renegotiation
url: https://datatracker.ietf.org/doc/html/rfc5746

Log (CVSS: 0.0)
NVT: SSL/TLS: Untrusted Certificate Detection

Summary
Checks and reports if a remote SSL/TLS service is using a certificate which is untrusted / the verification against the system wide trust store has failed.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
The remote SSL/TLS server is using the following certificate(s) which failed the
↪ verification against the system wide trust store (serial:issuer):
0CC5B263F56BB28519DD46EB06981D5225624BD1:C=DE,ST=Niedersachsen,L=Osnabrueck,O=Gr
↪eenbone AG Customer,OU=Vulnerability Management Team,CN=gsm.gbuser.net (Server
↪ certificate)
```

Solution:

Log Method
Details: SSL/TLS: Untrusted Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.117764
Version used: 2024-09-27T05:05:23Z

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

```
Header Name             | Header Value
------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪-----------------------------------------------------------------------------
Content-Security-Policy | default-src 'none'; object-src 'none'; base-uri 'none'
↪; connect-src 'self'; script-src 'self'; script-src-elem 'self' 'unsafe-inline
↪';frame-ancestors 'none'; form-action 'self'; style-src-elem 'self' 'unsafe-in
↪line'; style-src 'self' 'unsafe-inline'; font-src 'self';img-src 'self' blob
X-Content-Type-Options  | nosniff
X-Frame-Options         | SAMEORIGIN<newline>X-Frame-Options
X-XSS-Protection        | 1; mode=block
Missing Headers                   | More Information
------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪----------
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
Expect-CT                         | https://owasp.org/www-project-secure-headers
↪/#expect-ct, Note: This is an upcoming 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
Public-Key-Pins                   | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
```

... continues on next page ...

... continued from previous page ...

```
↪/#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
Strict-Transport-Security       | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
```

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: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

Summary
This routine identifies services supporting the following extensions to TLS:
- Application-Layer Protocol Negotiation (ALPN)
- Next Protocol Negotiation (NPN).
Based on the availability of this extensions the supported Network Protocols by this service are gathered and reported.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote service advertises support for the following Network Protocol(s) via the NPN extension:

... continues on next page ...

... continued from previous page ...

SSL/TLS Protocol:Network Protocol
TLSv1.2:HTTP/1.1
TLSv1.2:HTTP/2
The remote service advertises support for the following Network Protocol(s) via
↪the ALPN extension:
SSL/TLS Protocol:Network Protocol
TLSv1.2:HTTP/1.1
TLSv1.2:HTTP/2

Solution:

Log Method
Details: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
OID:1.3.6.1.4.1.25623.1.0.108099
Version used: 2024-09-27T05:05:23Z

References
url: https://tools.ietf.org/html/rfc7301
url: https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote HTTP Server banner is:
Server: nginx

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

Log (CVSS: 0.0)
NVT: HTTP Server Banner Enumeration

... continues on next page ...

... continued from previous page ...

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: nginx | Invalid HTTP 00.5 GET request (non-existent HTTP version) to '/'
```

Solution:

Log Method
Details: `HTTP Server Banner Enumeration`
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: `2025-01-31T15:39:24Z`

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 "192.168.2.108" 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.
The service is responding with a 200 HTTP status code to non-existent files/urls
↪. The following pattern is used to work around possible false detections:
-----
```

... continues on next page ...

... continued from previous page ...

```
Greenbone Enterprise Appliance
-----
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; 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:
https://192.168.2.108/
https://192.168.2.108/assets
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?/)"
https://192.168.2.108/img
```

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: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
A TLScustom server answered on this port

Solution:

... continues on next page ...

... continued from previous page ...

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: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

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

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: SSL/TLS: Version Detection

Summary
Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
The remote SSL/TLS service supports the following SSL/TLS protocol version(s):
TLSv1.2
TLSv1.3
```

Solution:

Log Method
Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers.
Details: `SSL/TLS: Version Detection`
OID:1.3.6.1.4.1.25623.1.0.105782
Version used: `2024-09-27T05:05:23Z`

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.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)              | D3C255C6D78958DDE7DAD760D290E990E4C02A08
fingerprint (SHA-256)            | 2033B1DCFC10EC3189B15C5E6CE7791BB257D53783A03B
↪55CBD9C612393B4860
issued by                        | C=DE,ST=Niedersachsen,L=Osnabrueck,O=Greenbone
↪ AG Customer,OU=Vulnerability Management Team,CN=gsm.gbuser.net
public key algorithm             | RSA
public key size (bits)           | 3072
serial                           | 0CC5B263F56BB28519DD46EB06981D5225624BD1
signature algorithm              | sha256WithRSAEncryption
subject                          | C=DE,ST=Niedersachsen,L=Osnabrueck,O=Greenbone
↪ AG Customer,OU=Vulnerability Management Team,CN=gsm.gbuser.net
subject alternative names (SAN)  | gsm.gbuser.net
valid from                       | 2025-02-07 07:40:09 UTC
valid until                      | 2027-02-07 07:40:09 UTC
```

Solution:

Log Method

... continues on next page ...

... continued from previous page ...

Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The service is responding with a 200 HTTP status code to non-existent files/urls ↪. The following pattern is used to work around possible false detections:

Greenbone Enterprise Appliance

Solution:

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, authentication page or redirect 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: 2023-07-07T05:05:26Z

Log (CVSS: 0.0)
NVT: Greenbone Security Assistant (GSA) Detection (HTTP)

... continues on next page ...

... continued from previous page ...

Summary
HTTP based detection of the Greenbone Security Assistant (GSA).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Detected Greenbone Security Assistant (GSA)
Version:        unknown
Location:       /
CPE:            cpe:/a:greenbone:greenbone_security_assistant
```

Solution:

Log Method
Details: `Greenbone Security Assistant (GSA) Detection (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.103841
Version used: `2024-06-12T05:05:44Z`

References
`url: https://github.com/greenbone/gsa`

[return to 192.168.2.108]

2.1.5 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
192.168.2.108|cpe:/a:f5:nginx
192.168.2.108|cpe:/a:greenbone:greenbone_security_assistant
192.168.2.108|cpe:/a:greenbone:gsm_trial
192.168.2.108|cpe:/a:ietf:transport_layer_security:1.2
192.168.2.108|cpe:/a:ietf:transport_layer_security:1.3
192.168.2.108|cpe:/a:nginx:nginx
```

... continues on next page ...

... continued from previous page ...

192.168.2.108	cpe:/o:greenbone:greenbone_os:22.04.27

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

[return to 192.168.2.108]

2.2 192.168.2.1

Host scan start Thu Mar 6 02:25:27 2025 UTC
Host scan end Thu Mar 6 05:58:13 2025 UTC

Service (Port)	Threat Level
443/tcp	High
80/tcp	High
9443/tcp	Medium
443/tcp	Medium
80/tcp	Medium
general/icmp	Low
general/CPE-T	Log
445/tcp	Log
53/tcp	Log
general/tcp	Log
9443/tcp	Log
443/tcp	Log
10080/tcp	Log
80/tcp	Log
9000/tcp	Log

2.2.1 High 443/tcp

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

Summary

... continues on next page ...

... continued from previous page ...

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

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
The "jQuery" version on the remote host has reached the end of life.
CPE:                cpe:/a:jquery:jquery:1.8.3
Installed version:  1.8.3
Location/URL:       /js/thirdParty/jquery-1.8.3.min.js
EOL version:        1
EOL date:           unknown
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file:  https://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at:    https://mynetwork.home/
```

Impact

An EOL version of jQuery is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:

Solution type: VendorFix

Update jQuery on the remote host to a still supported version.

Vulnerability Detection Method

Checks if an EOL version is present on the target host.

Details: `jQuery End of Life (EOL) Detection - Linux`

OID:1.3.6.1.4.1.25623.1.0.117149

Version used: `2024-02-28T14:37:42Z`

References

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

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

Product detection result

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

Summary

The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 30%

Vulnerability Detection Result
'DHE' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Impact
This vulnerability allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, also known as a D(HE)ater attack.
There could be an increase in CPU usage in the affected component. For OpenSSH, users may observe issues such as a slowdown in SSH connections.

Solution:
Solution type: Mitigation
- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered.
- Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
- CVE-2002-20001: The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.
- CVE-2022-40735: The Diffie-Hellman Key Agreement Protocol allows use of long exponents that arguably make certain calculations unnecessarily expensive, because the 1996 van Oorschot and Wiener paper found that '(appropriately) short exponents' can be used when there are adequate subgroup constraints, and these short exponents can lead to less expensive calculations than for long exponents. This issue is different from CVE-2002-20001 because it is based on an observation about exponent size, rather than an observation about numbers that are not public keys. The specific situations in which calculation expense would constitute a server-side vulnerability depend on the protocol (e.g., TLS, SSH, or IKE) and the DHE implementation details. In general, there might be an availability concern because of server-side resource consumption from DHE modular-exponentiation calculations. Finally, it is possible for an attacker to exploit this vulnerability and CVE-2002-20001 together.

... continues on next page ...

... continued from previous page ...

- CVE-2024-41996: Validating the order of the public keys in the Diffie-Hellman Key Agreement Protocol, when an approved safe prime is used, allows remote attackers (from the client side) to trigger unnecessarily expensive server-side DHE modular-exponentiation calculations. The client may cause asymmetric resource consumption. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE and validate the order of the public key.

Vulnerability Detection Method
Checks the supported cipher suites of the remote SSL/TLS server.
Details: `Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)`
OID:1.3.6.1.4.1.25623.1.0.117840
Version used: `2024-10-03T05:05:33Z`

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

References
`cve: CVE-2002-20001`
`cve: CVE-2022-40735`
`cve: CVE-2024-41996`
`url: https://dheatattack.gitlab.io/`
`url: https://dheatattack.gitlab.io/details/`
`url: https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Se`
`↪curity_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol`
`url: https://github.com/Balasys/dheater`
`url: https://github.com/c0r0n3r/dheater`
`cert-bund: WID-SEC-2024-3056`
`cert-bund: WID-SEC-2023-1886`
`cert-bund: WID-SEC-2023-1352`
`cert-bund: WID-SEC-2022-2251`
`cert-bund: WID-SEC-2022-2000`
`cert-bund: CB-K22/0224`
`cert-bund: CB-K21/1276`
`dfn-cert: DFN-CERT-2024-2847`
`dfn-cert: DFN-CERT-2024-2578`
`dfn-cert: DFN-CERT-2024-1671`
`dfn-cert: DFN-CERT-2023-1697`
`dfn-cert: DFN-CERT-2023-1332`
`dfn-cert: DFN-CERT-2022-2147`
`dfn-cert: DFN-CERT-2022-0437`
`dfn-cert: DFN-CERT-2021-2622`

[return to 192.168.2.1]

2.2.2 High 80/tcp

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

Summary
The jQuery version on the remote host has reached the end of life (EOL) and should not be used anymore.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
The "jQuery" version on the remote host has reached the end of life.
CPE:               cpe:/a:jquery:jquery:1.8.3
Installed version: 1.8.3
Location/URL:      /js/thirdParty/jquery-1.8.3.min.js
EOL version:       1
EOL date:          unknown
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at:   http://mynetwork.home/
```

Impact
An EOL version of jQuery is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:
Solution type: VendorFix
Update jQuery on the remote host to a still supported version.

Vulnerability Detection Method
Checks if an EOL version is present on the target host.
Details: `jQuery End of Life (EOL) Detection - Linux`
OID:1.3.6.1.4.1.25623.1.0.117149
Version used: `2024-02-28T14:37:42Z`

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

[return to 192.168.2.1]

2.2.3 Medium 9443/tcp

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

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

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

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

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

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

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

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

Product Detection Result
. . . continues on next page . . .

... continued from previous page ...

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

References

cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              CN=*,L=SanDiego,ST=California,OU=TwonkyServer,O=PacketVide
↪o,C=US
Signature Algorithm:  sha1WithRSAEncryption
```

Solution:
Solution type: Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

References
`url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/`

[return to 192.168.2.1]

2.2.4 Medium 443/tcp

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability via the load method.

Quality of Detection (QoD): 30%

Vulnerability Detection Result
```
Installed version: 1.8.3
Fixed version:     1.9.0
Installation
path / port:       /js/thirdParty/jquery-1.8.3.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: https://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at:   https://mynetwork.home/
```

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery versions prior to 1.9.0.

Vulnerability Insight
jQuery allows cross-site scripting attacks via the load method. The load method fails to recognize and remove '<script>' HTML tags that contain a whitespace character, i.e: '</script >', which results in the enclosed script logic to be executed.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.143968
Version used: `2023-07-14T05:06:08Z`

References
`cve: CVE-2020-7656`
`url: https://snyk.io/vuln/SNYK-JS-JQUERY-569619`
`cert-bund: WID-SEC-2023-0558`
`cert-bund: WID-SEC-2022-0736`
`dfn-cert: DFN-CERT-2022-1614`
`dfn-cert: DFN-CERT-2021-2348`
`dfn-cert: DFN-CERT-2021-1503`
`dfn-cert: DFN-CERT-2020-2259`
`dfn-cert: DFN-CERT-2020-2209`

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 1.8.3
Fixed version:     1.9.0
Installation
path / port:       /js/thirdParty/jquery-1.8.3.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: https://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
```

... continues on next page ...

... continued from previous page ...

- Referenced at: https://mynetwork.home/

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery < 1.9.0 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: 2023-07-14T05:06:08Z

References
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590

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

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

Quality of Detection (QoD): 30%

Vulnerability Detection Result
Installed version: 1.8.3
Fixed version: 3.4.0
Installation
path / port: /js/thirdParty/jquery-1.8.3.min.js

... continues on next page ...

... continued from previous page ...

```
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: https://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at:   https://mynetwork.home/
```

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

Affected Software/OS
jQuery prior to version 3.4.0.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 3.4.0 Object Extensions Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.142314
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2019-5428
cve: CVE-2019-11358
url: https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/
url: https://github.com/DanielRuf/snyk-js-jquery-174006?files=1
cert-bund: WID-SEC-2024-1872
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2023-0239
cert-bund: WID-SEC-2022-1948
cert-bund: WID-SEC-2022-1947
cert-bund: WID-SEC-2022-0732
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K21/1083
cert-bund: CB-K20/1049
cert-bund: CB-K20/1030
cert-bund: CB-K20/0800
cert-bund: CB-K20/0710
cert-bund: CB-K20/0324
cert-bund: CB-K20/0314
cert-bund: CB-K20/0309
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K20/0106
cert-bund: CB-K20/0041
cert-bund: CB-K20/0037
cert-bund: CB-K20/0034
cert-bund: CB-K19/0921
cert-bund: CB-K19/0920
cert-bund: CB-K19/0916
cert-bund: CB-K19/0911
cert-bund: CB-K19/0909
cert-bund: CB-K19/0619
cert-bund: CB-K19/0504
cert-bund: CB-K19/0329
dfn-cert: DFN-CERT-2024-1997
dfn-cert: DFN-CERT-2023-2027
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2023-0481
dfn-cert: DFN-CERT-2023-0245
dfn-cert: DFN-CERT-2022-2467
dfn-cert: DFN-CERT-2021-1536
dfn-cert: DFN-CERT-2021-1503
dfn-cert: DFN-CERT-2021-0826
dfn-cert: DFN-CERT-2020-2423
dfn-cert: DFN-CERT-2020-2335
dfn-cert: DFN-CERT-2020-2286
dfn-cert: DFN-CERT-2020-2130
dfn-cert: DFN-CERT-2020-1812
dfn-cert: DFN-CERT-2020-1574
dfn-cert: DFN-CERT-2020-1537
dfn-cert: DFN-CERT-2020-1506
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2020-0769
dfn-cert: DFN-CERT-2020-0721
dfn-cert: DFN-CERT-2020-0276
dfn-cert: DFN-CERT-2020-0102
dfn-cert: DFN-CERT-2020-0100
dfn-cert: DFN-CERT-2019-2169
dfn-cert: DFN-CERT-2019-2158
dfn-cert: DFN-CERT-2019-2156
dfn-cert: DFN-CERT-2019-2126
dfn-cert: DFN-CERT-2019-1861
dfn-cert: DFN-CERT-2019-1663
dfn-cert: DFN-CERT-2019-1460
dfn-cert: DFN-CERT-2019-1182
dfn-cert: DFN-CERT-2019-1153
dfn-cert: DFN-CERT-2019-1118
dfn-cert: DFN-CERT-2019-1033
dfn-cert: DFN-CERT-2019-0914

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2019-0899
dfn-cert: DFN-CERT-2019-0805

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

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 30%

Vulnerability Detection Result
Installed version: 1.8.3
Fixed version: 3.0.0
Installation
path / port: /js/thirdParty/jquery-1.8.3.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: https://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at: https://mynetwork.home/

Solution:
Solution type: VendorFix
Update to version 3.0.0 or later.

Affected Software/OS
jQuery prior to version 3.0.0.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery < 3.0.0 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141635
Version used: 2023-07-14T05:06:08Z

References
cve: CVE-2015-9251
url: https://github.com/jquery/jquery/issues/2432
cert-bund: WID-SEC-2024-1872
cert-bund: WID-SEC-2024-1682
cert-bund: WID-SEC-2023-0239
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K20/1030
cert-bund: CB-K20/0309
cert-bund: CB-K20/0041
cert-bund: CB-K19/0911
cert-bund: CB-K19/0909
cert-bund: CB-K19/0615
cert-bund: CB-K19/0321
cert-bund: CB-K19/0313
cert-bund: CB-K19/0054
cert-bund: CB-K19/0052
cert-bund: CB-K19/0049
cert-bund: CB-K19/0048
cert-bund: CB-K19/0046
cert-bund: CB-K18/1006
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2023-0245
dfn-cert: DFN-CERT-2020-2423
dfn-cert: DFN-CERT-2020-2130
dfn-cert: DFN-CERT-2020-0630
dfn-cert: DFN-CERT-2020-0590
dfn-cert: DFN-CERT-2020-0318
dfn-cert: DFN-CERT-2019-2158
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0777
dfn-cert: DFN-CERT-2019-0772
dfn-cert: DFN-CERT-2019-0119
dfn-cert: DFN-CERT-2019-0111
dfn-cert: DFN-CERT-2018-2103
dfn-cert: DFN-CERT-2018-1163
```

Medium (CVSS: 6.1)
NVT: jQuery 1.0.3 < 3.5.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability when appending HTML containing option elements.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
Installed version: 1.8.3
Fixed version:     3.5.0
Installation
path / port:       /js/thirdParty/jquery-1.8.3.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: https://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
```

... continues on next page ...

... continued from previous page ...

- Referenced at: https://mynetwork.home/

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

Affected Software/OS
jQuery versions starting from 1.0.3 and prior to version 3.5.0.

Vulnerability Insight
Passing HTML containing <option> elements from untrusted sources - even after sanitizing them - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery 1.0.3 < 3.5.0 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.143813
Version used: 2025-01-31T15:39:24Z

References
cve: CVE-2020-11023
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://github.com/jquery/jquery/security/advisories/GHSA-jpcq-cgw6-v4j6
url: https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
url: https://masatokinugawa.l0.cm/2020/05/jquery3.5.0-xss.html
url: https://security.snyk.io/vuln/SNYK-JS-JQUERY-565129
cert-bund: WID-SEC-2024-3191
cert-bund: WID-SEC-2024-1872
cert-bund: WID-SEC-2023-0239
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-1347
cert-bund: WID-SEC-2022-1189
cert-bund: WID-SEC-2022-0757
cert-bund: WID-SEC-2022-0732
cert-bund: CB-K21/1085
cert-bund: CB-K21/1067
cert-bund: CB-K21/0418
cert-bund: CB-K20/1049
cert-bund: CB-K20/1027
cert-bund: CB-K20/1025
cert-bund: CB-K20/1024
cert-bund: CB-K20/1021
cert-bund: CB-K20/1008
cert-bund: CB-K20/0870

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K20/0800
cert-bund: CB-K20/0705
cert-bund: CB-K20/0521
dfn-cert: DFN-CERT-2024-2743
dfn-cert: DFN-CERT-2023-2027
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2023-0481
dfn-cert: DFN-CERT-2023-0245
dfn-cert: DFN-CERT-2022-1988
dfn-cert: DFN-CERT-2022-1610
dfn-cert: DFN-CERT-2022-0119
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2021-2348
dfn-cert: DFN-CERT-2021-1687
dfn-cert: DFN-CERT-2021-1111
dfn-cert: DFN-CERT-2021-0820
dfn-cert: DFN-CERT-2021-0633
dfn-cert: DFN-CERT-2021-0563
dfn-cert: DFN-CERT-2021-0545
dfn-cert: DFN-CERT-2020-2776
dfn-cert: DFN-CERT-2020-2423
dfn-cert: DFN-CERT-2020-2335
dfn-cert: DFN-CERT-2020-2287
dfn-cert: DFN-CERT-2020-2227
dfn-cert: DFN-CERT-2020-2209
dfn-cert: DFN-CERT-2020-2074
dfn-cert: DFN-CERT-2020-1743
dfn-cert: DFN-CERT-2020-1712
dfn-cert: DFN-CERT-2020-1509
dfn-cert: DFN-CERT-2020-1506
dfn-cert: DFN-CERT-2020-1433
dfn-cert: DFN-CERT-2020-1163
dfn-cert: DFN-CERT-2020-1099
```

Medium (CVSS: 6.1)
NVT: jQuery 1.2 < 3.5.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability in jQuery.htmlPrefilter and related methods.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
Installed version: 1.8.3
Fixed version:     3.5.0
Installation
```

... continues on next page ...

... continued from previous page ...

```
path / port:       /js/thirdParty/jquery-1.8.3.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: https://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at:   https://mynetwork.home/
```

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

Affected Software/OS
jQuery versions starting from 1.2 and prior to version 3.5.0.

Vulnerability Insight
Passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery 1.2 < 3.5.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.143812
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2020-11022
url: https://github.com/jquery/jquery/security/advisories/GHSA-gxr4-xjj5-5px2
url: https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
url: https://masatokinugawa.l0.cm/2020/05/jquery3.5.0-xss.html
url: https://security.snyk.io/vuln/SNYK-JS-JQUERY-567880
cert-bund: WID-SEC-2024-3217
cert-bund: WID-SEC-2024-1872
cert-bund: WID-SEC-2023-0239
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1347
cert-bund: WID-SEC-2022-0740
cert-bund: WID-SEC-2022-0732
cert-bund: WID-SEC-2022-0624
cert-bund: CB-K22/0463
cert-bund: CB-K21/1085
cert-bund: CB-K21/0071
cert-bund: CB-K21/0070
cert-bund: CB-K21/0069
cert-bund: CB-K21/0067
cert-bund: CB-K21/0061
cert-bund: CB-K21/0059
cert-bund: CB-K20/1049
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K20/1030
cert-bund: CB-K20/1027
cert-bund: CB-K20/1025
cert-bund: CB-K20/1023
cert-bund: CB-K20/1008
cert-bund: CB-K20/0870
cert-bund: CB-K20/0800
cert-bund: CB-K20/0705
cert-bund: CB-K20/0521
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2023-2027
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2023-0481
dfn-cert: DFN-CERT-2023-0245
dfn-cert: DFN-CERT-2022-1988
dfn-cert: DFN-CERT-2022-1670
dfn-cert: DFN-CERT-2022-0869
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2021-2190
dfn-cert: DFN-CERT-2021-1111
dfn-cert: DFN-CERT-2021-0828
dfn-cert: DFN-CERT-2021-0826
dfn-cert: DFN-CERT-2021-0819
dfn-cert: DFN-CERT-2021-0633
dfn-cert: DFN-CERT-2021-0545
dfn-cert: DFN-CERT-2021-0140
dfn-cert: DFN-CERT-2021-0138
dfn-cert: DFN-CERT-2021-0135
dfn-cert: DFN-CERT-2021-0132
dfn-cert: DFN-CERT-2020-2423
dfn-cert: DFN-CERT-2020-2335
dfn-cert: DFN-CERT-2020-2305
dfn-cert: DFN-CERT-2020-2286
dfn-cert: DFN-CERT-2020-2227
dfn-cert: DFN-CERT-2020-2209
dfn-cert: DFN-CERT-2020-2130
dfn-cert: DFN-CERT-2020-2074
dfn-cert: DFN-CERT-2020-2015
dfn-cert: DFN-CERT-2020-2001
dfn-cert: DFN-CERT-2020-1838
dfn-cert: DFN-CERT-2020-1812
dfn-cert: DFN-CERT-2020-1712
dfn-cert: DFN-CERT-2020-1509
dfn-cert: DFN-CERT-2020-1506
dfn-cert: DFN-CERT-2020-1433
dfn-cert: DFN-CERT-2020-1163
dfn-cert: DFN-CERT-2020-1161

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-1138
dfn-cert: DFN-CERT-2020-1099

Medium (CVSS: 6.1)
NVT: jQuery 1.4.2 <= 1.11.0 XSS Vulnerability

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

Quality of Detection (QoD): 30%

Vulnerability Detection Result
Installed version: 1.8.3
Fixed version: 1.11.1
Installation
path / port: /js/thirdParty/jquery-1.8.3.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: https://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at: https://mynetwork.home/

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

Affected Software/OS
jQuery version 1.4.2 through 1.11.0.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery 1.4.2 <= 1.11.0 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.150660
Version used: 2023-07-14T05:06:08Z

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

Medium (CVSS: 5.0)
NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

... continues on next page ...

... continued from previous page ...

Summary
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪------------------------------------------------
TLSv1.2          | 10
```

Impact
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

Solution:
Solution type: VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

Affected Software/OS
Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

Vulnerability Insight
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

Vulnerability Detection Method
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: `2024-09-27T05:05:23Z`

References
```
cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego
```

... continues on next page ...

... continued from previous page ...

```
↪tiation-dos/
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
url: https://www.openwall.com/lists/oss-security/2011/07/08/2
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-0796
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K17/0980
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112
```

Medium (CVSS: 5.0)
NVT: Backup File Scanner (HTTP) - Unreliable Detection Reporting

Summary
The script reports backup files left on the web server.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
The following backup files were identified (<URL>:<Matching pattern>):
https://mynetwork.home/js/thirdParty/.pikaday.css.backup/.pikaday.css.backup:^HT
↪TP/1\.[01] 200
https://mynetwork.home/js/thirdParty/.pikaday.css.bak/.pikaday.css.bak:^HTTP/1\.
↪[01] 200
https://mynetwork.home/js/thirdParty/.pikaday.css.bkp/.pikaday.css.bkp:^HTTP/1\.
↪[01] 200
https://mynetwork.home/js/thirdParty/.pikaday.css.copy/.pikaday.css.copy:^HTTP/1
↪\.[01] 200
https://mynetwork.home/js/thirdParty/.pikaday.css.old/.pikaday.css.old:^HTTP/1\.
↪[01] 200
https://mynetwork.home/js/thirdParty/.pikaday.css.orig/.pikaday.css.orig:^HTTP/1
↪\.[01] 200
https://mynetwork.home/js/thirdParty/.pikaday.css.save/.pikaday.css.save:^HTTP/1
↪\.[01] 200
https://mynetwork.home/js/thirdParty/.pikaday.css.swp/.pikaday.css.swp:^HTTP/1\.
↪[01] 200
https://mynetwork.home/js/thirdParty/.pikaday.css.temp/.pikaday.css.temp:^HTTP/1
↪\.[01] 200
https://mynetwork.home/js/thirdParty/.pikaday.css.tmp/.pikaday.css.tmp:^HTTP/1\.
```

... continues on next page ...

... continued from previous page ...

```
↪[01] 200
https://mynetwork.home/js/thirdParty/.pikaday.css~/.pikaday.css~:^HTTP/1\.[01] 2
↪00
https://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.backup:^HTTP/1\.
↪[01] 200
https://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.bak:^HTTP/1\.[01
↪] 200
https://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.bkp:^HTTP/1\.[01
↪] 200
https://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.copy:^HTTP/1\.[0
↪1] 200
https://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.old:^HTTP/1\.[01
↪] 200
https://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.orig:^HTTP/1\.[0
↪1] 200
https://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.save:^HTTP/1\.[0
↪1] 200
https://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.swp:^HTTP/1\.[01
↪] 200
https://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.temp:^HTTP/1\.[0
↪1] 200
https://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.tmp:^HTTP/1\.[01
↪] 200
https://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css~:^HTTP/1\.[01] 2
↪00
https://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.backup:^HTTP/1\.[
↪01] 200
https://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.bak:^HTTP/1\.[01]
↪ 200
https://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.bkp:^HTTP/1\.[01]
↪ 200
https://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.copy:^HTTP/1\.[01
↪] 200
https://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.old:^HTTP/1\.[01]
↪ 200
https://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.orig:^HTTP/1\.[01
↪] 200
https://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.save:^HTTP/1\.[01
↪] 200
https://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.swp:^HTTP/1\.[01]
↪ 200
https://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.temp:^HTTP/1\.[01
↪] 200
https://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.tmp:^HTTP/1\.[01]
↪ 200
https://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css~:^HTTP/1\.[01] 20
↪0
```

... continues on next page ...

... continued from previous page ...

```
https://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.backup:^HTTP/1\.[01]
↪ 200
https://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.bak:^HTTP/1\.[01] 20
↪0
https://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.bkp:^HTTP/1\.[01] 20
↪0
https://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.copy:^HTTP/1\.[01] 2
↪00
https://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.old:^HTTP/1\.[01] 20
↪0
https://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.orig:^HTTP/1\.[01] 2
↪00
https://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.save:^HTTP/1\.[01] 2
↪00
https://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.swp:^HTTP/1\.[01] 20
↪0
https://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.temp:^HTTP/1\.[01] 2
↪00
https://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.tmp:^HTTP/1\.[01] 20
↪0
https://mynetwork.home/js/thirdParty/pikaday/css/.theme.css~:^HTTP/1\.[01] 200
https://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.backup:^HTTP/1\.[01
↪] 200
https://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.bak:^HTTP/1\.[01] 2
↪00
https://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.bkp:^HTTP/1\.[01] 2
↪00
https://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.copy:^HTTP/1\.[01]
↪200
https://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.old:^HTTP/1\.[01] 2
↪00
https://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.orig:^HTTP/1\.[01]
↪200
https://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.save:^HTTP/1\.[01]
↪200
https://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.swp:^HTTP/1\.[01] 2
↪00
https://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.temp:^HTTP/1\.[01]
↪200
https://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.tmp:^HTTP/1\.[01] 2
↪00
https://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css~:^HTTP/1\.[01] 200
https://mynetwork.home/js/thirdParty/pikaday/css/theme.css.backup:^HTTP/1\.[01]
↪200
https://mynetwork.home/js/thirdParty/pikaday/css/theme.css.bak:^HTTP/1\.[01] 200
https://mynetwork.home/js/thirdParty/pikaday/css/theme.css.bkp:^HTTP/1\.[01] 200
https://mynetwork.home/js/thirdParty/pikaday/css/theme.css.copy:^HTTP/1\.[01] 20
```

... continues on next page ...

... continued from previous page ...

```
↪0
https://mynetwork.home/js/thirdParty/pikaday/css/theme.css.old:^HTTP/1\.[01] 200
https://mynetwork.home/js/thirdParty/pikaday/css/theme.css.orig:^HTTP/1\.[01] 20
↪0
https://mynetwork.home/js/thirdParty/pikaday/css/theme.css.save:^HTTP/1\.[01] 20
↪0
https://mynetwork.home/js/thirdParty/pikaday/css/theme.css.swp:^HTTP/1\.[01] 200
https://mynetwork.home/js/thirdParty/pikaday/css/theme.css.temp:^HTTP/1\.[01] 20
↪0
https://mynetwork.home/js/thirdParty/pikaday/css/theme.css.tmp:^HTTP/1\.[01] 200
https://mynetwork.home/js/thirdParty/pikaday/css/theme.css~:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/.desktop.css.backup:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/.desktop.css.bak:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/.desktop.css.bkp:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/.desktop.css.copy:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/.desktop.css.old:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/.desktop.css.orig:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/.desktop.css.save:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/.desktop.css.swp:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/.desktop.css.temp:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/.desktop.css.tmp:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/.desktop.css~:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/desktop.css.backup:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/desktop.css.bak:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/desktop.css.bkp:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/desktop.css.copy:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/desktop.css.old:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/desktop.css.orig:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/desktop.css.save:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/desktop.css.swp:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/desktop.css.temp:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/desktop.css.tmp:^HTTP/1\.[01] 200
https://mynetwork.home/layout/css/desktop/desktop.css~:^HTTP/1\.[01] 200
```

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

Solution:
Solution type: Mitigation
Delete the backup files.

Vulnerability Insight
Notes:
- 'Unreliable Detection' means that a file was detected only based on a HTTP 200 (Found) status code reported by the remote web server when a file was requested.

... continues on next page ...

... continued from previous page ...

- As the VT 'Backup File Scanner (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.140853) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

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

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

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

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

Quality of Detection (QoD): 80%

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

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

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

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

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2024-09-30T08:38:05Z`

... continues on next page ...

... continued from previous page ...

References
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html

[return to 192.168.2.1]

2.2.5 Medium 80/tcp

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 1.8.3
Fixed version: 1.9.0
Installation
path / port: /js/thirdParty/jquery-1.8.3.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at: http://mynetwork.home/

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery < 1.9.0 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141636

... continues on next page ...

... continued from previous page ...

Version used: 2023-07-14T05:06:08Z

References
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590

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

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 30%

Vulnerability Detection Result
Installed version: 1.8.3
Fixed version: 3.0.0
Installation
path / port: /js/thirdParty/jquery-1.8.3.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at: http://mynetwork.home/

Solution:
Solution type: VendorFix
Update to version 3.0.0 or later.

Affected Software/OS
jQuery prior to version 3.0.0.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery < 3.0.0 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141635
Version used: 2023-07-14T05:06:08Z

... continues on next page ...

... continued from previous page ...

References

cve: CVE-2015-9251
url: https://github.com/jquery/jquery/issues/2432
cert-bund: WID-SEC-2024-1872
cert-bund: WID-SEC-2024-1682
cert-bund: WID-SEC-2023-0239
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K20/1030
cert-bund: CB-K20/0309
cert-bund: CB-K20/0041
cert-bund: CB-K19/0911
cert-bund: CB-K19/0909
cert-bund: CB-K19/0615
cert-bund: CB-K19/0321
cert-bund: CB-K19/0313
cert-bund: CB-K19/0054
cert-bund: CB-K19/0052
cert-bund: CB-K19/0049
cert-bund: CB-K19/0048
cert-bund: CB-K19/0046
cert-bund: CB-K18/1006
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2023-0245
dfn-cert: DFN-CERT-2020-2423
dfn-cert: DFN-CERT-2020-2130
dfn-cert: DFN-CERT-2020-0630
dfn-cert: DFN-CERT-2020-0590
dfn-cert: DFN-CERT-2020-0318
dfn-cert: DFN-CERT-2019-2158
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0777
dfn-cert: DFN-CERT-2019-0772
dfn-cert: DFN-CERT-2019-0119
dfn-cert: DFN-CERT-2019-0111
dfn-cert: DFN-CERT-2018-2103
dfn-cert: DFN-CERT-2018-1163

Medium (CVSS: 6.1)
NVT: jQuery 1.0.3 < 3.5.0 XSS Vulnerability

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability when appending HTML containing option elements.

Quality of Detection (QoD): 30%

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Installed version: 1.8.3
Fixed version:     3.5.0
Installation
path / port:       /js/thirdParty/jquery-1.8.3.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at:   http://mynetwork.home/
```

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

Affected Software/OS
jQuery versions starting from 1.0.3 and prior to version 3.5.0.

Vulnerability Insight
Passing HTML containing <option> elements from untrusted sources - even after sanitizing them - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery 1.0.3 < 3.5.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.143813
Version used: `2025-01-31T15:39:24Z`

References

```
cve: CVE-2020-11023
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://github.com/jquery/jquery/security/advisories/GHSA-jpcq-cgw6-v4j6
url: https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
url: https://masatokinugawa.l0.cm/2020/05/jquery3.5.0-xss.html
url: https://security.snyk.io/vuln/SNYK-JS-JQUERY-565129
cert-bund: WID-SEC-2024-3191
cert-bund: WID-SEC-2024-1872
cert-bund: WID-SEC-2023-0239
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-1347
cert-bund: WID-SEC-2022-1189
cert-bund: WID-SEC-2022-0757
cert-bund: WID-SEC-2022-0732
cert-bund: CB-K21/1085
cert-bund: CB-K21/1067
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K21/0418
cert-bund: CB-K20/1049
cert-bund: CB-K20/1027
cert-bund: CB-K20/1025
cert-bund: CB-K20/1024
cert-bund: CB-K20/1021
cert-bund: CB-K20/1008
cert-bund: CB-K20/0870
cert-bund: CB-K20/0800
cert-bund: CB-K20/0705
cert-bund: CB-K20/0521
dfn-cert: DFN-CERT-2024-2743
dfn-cert: DFN-CERT-2023-2027
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2023-0481
dfn-cert: DFN-CERT-2023-0245
dfn-cert: DFN-CERT-2022-1988
dfn-cert: DFN-CERT-2022-1610
dfn-cert: DFN-CERT-2022-0119
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2021-2348
dfn-cert: DFN-CERT-2021-1687
dfn-cert: DFN-CERT-2021-1111
dfn-cert: DFN-CERT-2021-0820
dfn-cert: DFN-CERT-2021-0633
dfn-cert: DFN-CERT-2021-0563
dfn-cert: DFN-CERT-2021-0545
dfn-cert: DFN-CERT-2020-2776
dfn-cert: DFN-CERT-2020-2423
dfn-cert: DFN-CERT-2020-2335
dfn-cert: DFN-CERT-2020-2287
dfn-cert: DFN-CERT-2020-2227
dfn-cert: DFN-CERT-2020-2209
dfn-cert: DFN-CERT-2020-2074
dfn-cert: DFN-CERT-2020-1743
dfn-cert: DFN-CERT-2020-1712
dfn-cert: DFN-CERT-2020-1509
dfn-cert: DFN-CERT-2020-1506
dfn-cert: DFN-CERT-2020-1433
dfn-cert: DFN-CERT-2020-1163
dfn-cert: DFN-CERT-2020-1099
```

Medium (CVSS: 6.1)
NVT: jQuery 1.2 < 3.5.0 XSS Vulnerability

Summary

... continues on next page ...

... continued from previous page ...

jQuery is prone to a cross-site scripting (XSS) vulnerability in jQuery.htmlPrefilter and related methods.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
Installed version: 1.8.3
Fixed version:     3.5.0
Installation
path / port:       /js/thirdParty/jquery-1.8.3.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at:   http://mynetwork.home/
```

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

Affected Software/OS
jQuery versions starting from 1.2 and prior to version 3.5.0.

Vulnerability Insight
Passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery 1.2 < 3.5.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.143812
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2020-11022
url: https://github.com/jquery/jquery/security/advisories/GHSA-gxr4-xjj5-5px2
url: https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
url: https://masatokinugawa.l0.cm/2020/05/jquery3.5.0-xss.html
url: https://security.snyk.io/vuln/SNYK-JS-JQUERY-567880
cert-bund: WID-SEC-2024-3217
cert-bund: WID-SEC-2024-1872
cert-bund: WID-SEC-2023-0239
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1347
cert-bund: WID-SEC-2022-0740
cert-bund: WID-SEC-2022-0732
cert-bund: WID-SEC-2022-0624
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K22/0463
cert-bund: CB-K21/1085
cert-bund: CB-K21/0071
cert-bund: CB-K21/0070
cert-bund: CB-K21/0069
cert-bund: CB-K21/0067
cert-bund: CB-K21/0061
cert-bund: CB-K21/0059
cert-bund: CB-K20/1049
cert-bund: CB-K20/1030
cert-bund: CB-K20/1027
cert-bund: CB-K20/1025
cert-bund: CB-K20/1023
cert-bund: CB-K20/1008
cert-bund: CB-K20/0870
cert-bund: CB-K20/0800
cert-bund: CB-K20/0705
cert-bund: CB-K20/0521
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2023-2027
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2023-0481
dfn-cert: DFN-CERT-2023-0245
dfn-cert: DFN-CERT-2022-1988
dfn-cert: DFN-CERT-2022-1670
dfn-cert: DFN-CERT-2022-0869
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2021-2190
dfn-cert: DFN-CERT-2021-1111
dfn-cert: DFN-CERT-2021-0828
dfn-cert: DFN-CERT-2021-0826
dfn-cert: DFN-CERT-2021-0819
dfn-cert: DFN-CERT-2021-0633
dfn-cert: DFN-CERT-2021-0545
dfn-cert: DFN-CERT-2021-0140
dfn-cert: DFN-CERT-2021-0138
dfn-cert: DFN-CERT-2021-0135
dfn-cert: DFN-CERT-2021-0132
dfn-cert: DFN-CERT-2020-2423
dfn-cert: DFN-CERT-2020-2335
dfn-cert: DFN-CERT-2020-2305
dfn-cert: DFN-CERT-2020-2286
dfn-cert: DFN-CERT-2020-2227
dfn-cert: DFN-CERT-2020-2209
dfn-cert: DFN-CERT-2020-2130
dfn-cert: DFN-CERT-2020-2074
dfn-cert: DFN-CERT-2020-2015

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2020-2001
dfn-cert: DFN-CERT-2020-1838
dfn-cert: DFN-CERT-2020-1812
dfn-cert: DFN-CERT-2020-1712
dfn-cert: DFN-CERT-2020-1509
dfn-cert: DFN-CERT-2020-1506
dfn-cert: DFN-CERT-2020-1433
dfn-cert: DFN-CERT-2020-1163
dfn-cert: DFN-CERT-2020-1161
dfn-cert: DFN-CERT-2020-1138
dfn-cert: DFN-CERT-2020-1099
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability via the load method.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
Installed version: 1.8.3
Fixed version:     1.9.0
Installation
path / port:       /js/thirdParty/jquery-1.8.3.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at:   http://mynetwork.home/
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery versions prior to 1.9.0.

Vulnerability Insight
jQuery allows cross-site scripting attacks via the load method. The load method fails to recognize and remove '<script>' HTML tags that contain a whitespace character, i.e: '</script >', which results in the enclosed script logic to be executed.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.143968

... continues on next page ...

... continued from previous page ...

Version used: 2023-07-14T05:06:08Z

References
cve: CVE-2020-7656
url: https://snyk.io/vuln/SNYK-JS-JQUERY-569619
cert-bund: WID-SEC-2023-0558
cert-bund: WID-SEC-2022-0736
dfn-cert: DFN-CERT-2022-1614
dfn-cert: DFN-CERT-2021-2348
dfn-cert: DFN-CERT-2021-1503
dfn-cert: DFN-CERT-2020-2259
dfn-cert: DFN-CERT-2020-2209

Medium (CVSS: 6.1)
NVT: jQuery 1.4.2 <= 1.11.0 XSS Vulnerability

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

Quality of Detection (QoD): 30%

Vulnerability Detection Result
Installed version: 1.8.3
Fixed version: 1.11.1
Installation
path / port: /js/thirdParty/jquery-1.8.3.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at: http://mynetwork.home/

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

Affected Software/OS
jQuery version 1.4.2 through 1.11.0.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery 1.4.2 <= 1.11.0 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.150660

... continues on next page ...

... continued from previous page ...

Version used: 2023-07-14T05:06:08Z

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

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

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

Quality of Detection (QoD): 30%

Vulnerability Detection Result
Installed version: 1.8.3
Fixed version: 3.4.0
Installation
path / port: /js/thirdParty/jquery-1.8.3.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at: http://mynetwork.home/

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

Affected Software/OS
jQuery prior to version 3.4.0.

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery < 3.4.0 Object Extensions Vulnerability
OID:1.3.6.1.4.1.25623.1.0.142314
Version used: 2023-07-14T05:06:08Z

References

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2019-5428
cve: CVE-2019-11358
url: https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/
url: https://github.com/DanielRuf/snyk-js-jquery-174006?files=1
cert-bund: WID-SEC-2024-1872
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2023-0239
cert-bund: WID-SEC-2022-1948
cert-bund: WID-SEC-2022-1947
cert-bund: WID-SEC-2022-0732
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K21/1083
cert-bund: CB-K20/1049
cert-bund: CB-K20/1030
cert-bund: CB-K20/0800
cert-bund: CB-K20/0710
cert-bund: CB-K20/0324
cert-bund: CB-K20/0314
cert-bund: CB-K20/0309
cert-bund: CB-K20/0106
cert-bund: CB-K20/0041
cert-bund: CB-K20/0037
cert-bund: CB-K20/0034
cert-bund: CB-K19/0921
cert-bund: CB-K19/0920
cert-bund: CB-K19/0916
cert-bund: CB-K19/0911
cert-bund: CB-K19/0909
cert-bund: CB-K19/0619
cert-bund: CB-K19/0504
cert-bund: CB-K19/0329
dfn-cert: DFN-CERT-2024-1997
dfn-cert: DFN-CERT-2023-2027
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2023-0481
dfn-cert: DFN-CERT-2023-0245
dfn-cert: DFN-CERT-2022-2467
dfn-cert: DFN-CERT-2021-1536
dfn-cert: DFN-CERT-2021-1503
dfn-cert: DFN-CERT-2021-0826
dfn-cert: DFN-CERT-2020-2423
dfn-cert: DFN-CERT-2020-2335
dfn-cert: DFN-CERT-2020-2286
dfn-cert: DFN-CERT-2020-2130
dfn-cert: DFN-CERT-2020-1812
dfn-cert: DFN-CERT-2020-1574
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2020-1537
dfn-cert: DFN-CERT-2020-1506
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2020-0769
dfn-cert: DFN-CERT-2020-0721
dfn-cert: DFN-CERT-2020-0276
dfn-cert: DFN-CERT-2020-0102
dfn-cert: DFN-CERT-2020-0100
dfn-cert: DFN-CERT-2019-2169
dfn-cert: DFN-CERT-2019-2158
dfn-cert: DFN-CERT-2019-2156
dfn-cert: DFN-CERT-2019-2126
dfn-cert: DFN-CERT-2019-1861
dfn-cert: DFN-CERT-2019-1663
dfn-cert: DFN-CERT-2019-1460
dfn-cert: DFN-CERT-2019-1182
dfn-cert: DFN-CERT-2019-1153
dfn-cert: DFN-CERT-2019-1118
dfn-cert: DFN-CERT-2019-1033
dfn-cert: DFN-CERT-2019-0914
dfn-cert: DFN-CERT-2019-0899
dfn-cert: DFN-CERT-2019-0805
```

Medium (CVSS: 5.0)
NVT: Backup File Scanner (HTTP) - Unreliable Detection Reporting

Summary
The script reports backup files left on the web server.

Quality of Detection (QoD): 30%

Vulnerability Detection Result

```
The following backup files were identified (<URL>:<Matching pattern>):
http://mynetwork.home/js/thirdParty/.pikaday.css.backup/.pikaday.css.backup:^HTT
↪P/1\.[01] 200
http://mynetwork.home/js/thirdParty/.pikaday.css.bak/.pikaday.css.bak:^HTTP/1\.[
↪01] 200
http://mynetwork.home/js/thirdParty/.pikaday.css.bkp/.pikaday.css.bkp:^HTTP/1\.[
↪01] 200
http://mynetwork.home/js/thirdParty/.pikaday.css.copy/.pikaday.css.copy:^HTTP/1\
↪.[01] 200
http://mynetwork.home/js/thirdParty/.pikaday.css.old/.pikaday.css.old:^HTTP/1\.[
↪01] 200
http://mynetwork.home/js/thirdParty/.pikaday.css.orig/.pikaday.css.orig:^HTTP/1\
↪.[01] 200
http://mynetwork.home/js/thirdParty/.pikaday.css.save/.pikaday.css.save:^HTTP/1\
↪.[01] 200
```

... continues on next page ...

... continued from previous page ...

```
http://mynetwork.home/js/thirdParty/.pikaday.css.swp/.pikaday.css.swp:^HTTP/1\.[
↪01] 200
http://mynetwork.home/js/thirdParty/.pikaday.css.temp/.pikaday.css.temp:^HTTP/1\
↪.[01] 200
http://mynetwork.home/js/thirdParty/.pikaday.css.tmp/.pikaday.css.tmp:^HTTP/1\.[
↪01] 200
http://mynetwork.home/js/thirdParty/.pikaday.css~/.pikaday.css~:^HTTP/1\.[01] 20
↪0
http://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.backup:^HTTP/1\.[
↪01] 200
http://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.bak:^HTTP/1\.[01]
↪ 200
http://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.bkp:^HTTP/1\.[01]
↪ 200
http://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.copy:^HTTP/1\.[01
↪] 200
http://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.old:^HTTP/1\.[01]
↪ 200
http://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.orig:^HTTP/1\.[01
↪] 200
http://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.save:^HTTP/1\.[01
↪] 200
http://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.swp:^HTTP/1\.[01]
↪ 200
http://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.temp:^HTTP/1\.[01
↪] 200
http://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css.tmp:^HTTP/1\.[01]
↪ 200
http://mynetwork.home/js/thirdParty/noUiSlider/.nouislider.css~:^HTTP/1\.[01] 20
↪0
http://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.backup:^HTTP/1\.[0
↪1] 200
http://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.bak:^HTTP/1\.[01]
↪200
http://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.bkp:^HTTP/1\.[01]
↪200
http://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.copy:^HTTP/1\.[01]
↪ 200
http://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.old:^HTTP/1\.[01]
↪200
http://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.orig:^HTTP/1\.[01]
↪ 200
http://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.save:^HTTP/1\.[01]
↪ 200
http://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.swp:^HTTP/1\.[01]
↪200
http://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.temp:^HTTP/1\.[01]
```

... continues on next page ...

... continued from previous page ...

```
↪ 200
http://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css.tmp:^HTTP/1\.[01]
↪200
http://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css~:^HTTP/1\.[01] 200
http://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.backup:^HTTP/1\.[01]
↪200
http://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.bak:^HTTP/1\.[01] 200
http://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.bkp:^HTTP/1\.[01] 200
http://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.copy:^HTTP/1\.[01] 20
↪0
http://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.old:^HTTP/1\.[01] 200
http://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.orig:^HTTP/1\.[01] 20
↪0
http://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.save:^HTTP/1\.[01] 20
↪0
http://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.swp:^HTTP/1\.[01] 200
http://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.temp:^HTTP/1\.[01] 20
↪0
http://mynetwork.home/js/thirdParty/pikaday/css/.theme.css.tmp:^HTTP/1\.[01] 200
http://mynetwork.home/js/thirdParty/pikaday/css/.theme.css~:^HTTP/1\.[01] 200
http://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.backup:^HTTP/1\.[01]
↪ 200
http://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.bak:^HTTP/1\.[01] 20
↪0
http://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.bkp:^HTTP/1\.[01] 20
↪0
http://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.copy:^HTTP/1\.[01] 2
↪00
http://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.old:^HTTP/1\.[01] 20
↪0
http://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.orig:^HTTP/1\.[01] 2
↪00
http://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.save:^HTTP/1\.[01] 2
↪00
http://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.swp:^HTTP/1\.[01] 20
↪0
http://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.temp:^HTTP/1\.[01] 2
↪00
http://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css.tmp:^HTTP/1\.[01] 20
↪0
http://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css~:^HTTP/1\.[01] 200
http://mynetwork.home/js/thirdParty/pikaday/css/theme.css.backup:^HTTP/1\.[01] 2
↪00
http://mynetwork.home/js/thirdParty/pikaday/css/theme.css.bak:^HTTP/1\.[01] 200
http://mynetwork.home/js/thirdParty/pikaday/css/theme.css.bkp:^HTTP/1\.[01] 200
http://mynetwork.home/js/thirdParty/pikaday/css/theme.css.copy:^HTTP/1\.[01] 200
http://mynetwork.home/js/thirdParty/pikaday/css/theme.css.old:^HTTP/1\.[01] 200
```

... continues on next page ...

... continued from previous page ...

http://mynetwork.home/js/thirdParty/pikaday/css/theme.css.orig:^HTTP/1\.[01] 200
http://mynetwork.home/js/thirdParty/pikaday/css/theme.css.save:^HTTP/1\.[01] 200
http://mynetwork.home/js/thirdParty/pikaday/css/theme.css.swp:^HTTP/1\.[01] 200
http://mynetwork.home/js/thirdParty/pikaday/css/theme.css.temp:^HTTP/1\.[01] 200
http://mynetwork.home/js/thirdParty/pikaday/css/theme.css.tmp:^HTTP/1\.[01] 200
http://mynetwork.home/js/thirdParty/pikaday/css/theme.css~:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/.desktop.css.backup:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/.desktop.css.bak:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/.desktop.css.bkp:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/.desktop.css.copy:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/.desktop.css.old:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/.desktop.css.orig:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/.desktop.css.save:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/.desktop.css.swp:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/.desktop.css.temp:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/.desktop.css.tmp:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/.desktop.css~:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/desktop.css.backup:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/desktop.css.bak:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/desktop.css.bkp:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/desktop.css.copy:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/desktop.css.old:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/desktop.css.orig:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/desktop.css.save:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/desktop.css.swp:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/desktop.css.temp:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/desktop.css.tmp:^HTTP/1\.[01] 200
http://mynetwork.home/layout/css/desktop/desktop.css~:^HTTP/1\.[01] 200

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

Solution:
Solution type: Mitigation
Delete the backup files.

Vulnerability Insight
Notes:
- 'Unreliable Detection' means that a file was detected only based on a HTTP 200 (Found) status code reported by the remote web server when a file was requested.
- As the VT 'Backup File Scanner (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.140853) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method
Reports previous enumerated backup files accessible on the remote web server.

... continues on next page ...

... continued from previous page ...

Details: Backup File Scanner (HTTP) - Unreliable Detection Reporting
OID:1.3.6.1.4.1.25623.1.0.108975
Version used: 2022-09-13T10:15:09Z

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

[return to 192.168.2.1]

2.2.6 Low general/icmp

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

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0

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

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

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

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: ICMP Timestamp Reply Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.103190

... continues on next page ...

... continued from previous page ...

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 192.168.2.1]

2.2.7 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
192.168.2.1|cpe:/a:ietf:transport_layer_security:1.0
192.168.2.1|cpe:/a:ietf:transport_layer_security:1.2
192.168.2.1|cpe:/a:ietf:transport_layer_security:1.3
192.168.2.1|cpe:/a:jquery:jquery:1.8.3
192.168.2.1|cpe:/o:linux:kernel:2.x.x

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

[return to 192.168.2.1]

2.2.8 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: SMBv1 Enabled - Active Check
Summary The host has enabled SMBv1 for the SMB Server.
Quality of Detection (QoD): 80%
Vulnerability Detection Result `SMBv1 is enabled for the SMB Server`
Solution:
Log Method Checks if SMBv1 is enabled for the SMB Server based on the information provided by the following VT: - SMB Remote Version Detection (OID: 1.3.6.1.4.1.25623.1.0.807830). Details: `SMBv1 Enabled - Active Check` OID:1.3.6.1.4.1.25623.1.0.140151 Version used: `2024-01-09T05:06:46Z`
References `url: https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-`

... continues on next page ...

... continued from previous page ...

↪Practices
url: https://support.microsoft.com/en-us/kb/2696547
url: https://support.microsoft.com/en-us/kb/204279

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%

Vulnerability Detection Result
SMBv1, 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

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

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`

[return to 192.168.2.1]

2.2.9 Log 53/tcp

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:
UNKNOWN

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 192.168.2.1]

2.2.10 Log general/tcp

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:           Linux 2.x.x
Version:      2.x.x
CPE:          cpe:/o:linux:kernel:2.x.x
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 9000/tcp: Server: Linux/2.x.x, UPnP/1.
↪0, pvConnect UPnP SDK/1.0, Twonky UPnP SDK/1.1
Setting key "Host/runs_unixoide" based on this information
```

... 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: IP Forwarding Enabled - Active Check

Summary
Checks if the remote host has IP forwarding enabled.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
`It was possible to route a TCP packet through the target host and received an an`
`↪swer which means IP forwarding is enabled.`

Solution:

Log Method
Sends a crafted Local Link Layer (LLL) frame and checks the response.
Details: `IP Forwarding Enabled - Active Check`
OID:1.3.6.1.4.1.25623.1.0.147205
Version used: `2021-12-03T08:27:06Z`

References
`cve: CVE-1999-0511`

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This VT consolidates and reports the information collected by the following VTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

... continues on next page ...

... continued from previous page ...

If you know any of the information reported here, please send the full output to the referenced community forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Unknown banners have been collected which might help to identify the OS running
↪on this host. If these banners containing information about the host OS please
↪ report the following information to https://forum.greenbone.net/c/vulnerabili
↪ty-tests/7:
Banner: UNKNOWN
Identified from: DNS server banner on port 53/tcp
Banner: Server: HTTP Server
Identified from: HTTP Server banner on port 10080/tcp
Banner: Server: HTTP Server
Identified from: HTTP Server banner on port 443/tcp
Banner: Server: HTTP Server
Identified from: HTTP Server banner on port 80/tcp
```

Solution:

Log Method

Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `2023-06-22T10:34:15Z`

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 (192.168.2.108) to target (192.168.2.1):
192.168.2.108
192.168.2.1
Network distance between scanner and target: 2
```

Solution:

... continues on next page ...

... continued from previous page ...

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`

Log (CVSS: 0.0)
NVT: jQuery Detection Consolidation

Summary
Consolidation of jQuery detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected jQuery
Version:       1.8.3
Location:      /js/thirdParty/jquery-1.8.3.min.js
CPE:           cpe:/a:jquery:jquery:1.8.3
Concluded from version/product identification result:
src="/js/thirdParty/jquery-1.8.3.min.js
Concluded from version/product identification location:
- Identified file: https://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at:   https://mynetwork.home/
Detected jQuery
Version:       1.8.3
Location:      /js/thirdParty/jquery-1.8.3.min.js
CPE:           cpe:/a:jquery:jquery:1.8.3
Concluded from version/product identification result:
src="/js/thirdParty/jquery-1.8.3.min.js
Concluded from version/product identification location:
- Identified file: http://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js
- Referenced at:   http://mynetwork.home/
```

Solution:

Log Method
Details: `jQuery Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.150658

... continues on next page ...

... continued from previous page ...

Version used: 2023-07-14T05:06:08Z

References
url: https://jquery.com/

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 192.168.2.1:
Hostname|Source
mynetwork.home|Reverse-DNS

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: 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.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
The following additional but not resolvable hostnames were detected:
self-signedkey

Solution:

Log Method
Details: SSL/TLS: Hostname discovery from server certificate
OID:1.3.6.1.4.1.25623.1.0.111010

... continues on next page ...

... continued from previous page ...

Version used: 2021-11-22T15:32:39Z

[return to 192.168.2.1]

2.2.11 Log 9443/tcp

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This VT consolidates and reports the information collected by the following VTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)
If you know any of the information reported here, please send the full output to the referenced community forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
An unknown service is running on this port. If you know this service, please rep
↪ort the following information to https://forum.greenbone.net/c/vulnerability-t
↪ests/7:
Method: get_httpHex
0x00:  15 03 01 00 02 02 28 15 03 01 00 02 02 00          ......(.......
Nmap service detection (unknown) result for this port: ssl|tungsten-https
This is a guess. A confident identification of the service was not possible.
Hint: If you're running a recent nmap version try to run nmap with the following
↪ command: 'nmap -sV -Pn -p 9443 192.168.2.1' and submit a possible collected f
↪ingerprint to the nmap database.
```

Solution:

Log Method
Details: Unknown OS and Service Banner Reporting
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: 2023-06-22T10:34:15Z

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

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.

Quality of Detection (QoD): 98%

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

Solution:

Log Method
Details: `SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing`
OID:1.3.6.1.4.1.25623.1.0.105092
Version used: `2024-09-27T05:05:23Z`

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

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
```
No 'Strong' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Medium' cipher suites accepted by this service via the TLSv1.0 protocol.
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.
```

Solution:

Vulnerability Insight
Notes:
- As the VT '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 VT instead.
- SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Log Method

. . . continues on next page . . .

... continued from previous page ...

Details: SSL/TLS: Report Supported Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Safe/Secure Renegotiation Support Status

Summary
Checks and reports if a remote SSL/TLS service supports safe/secure renegotiation.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
Protocol Version | Safe/Secure Renegotiation Support Status
------------------------------------------------------------------------------
↪--
SSLv3            | Unknown, Reason: Failed to open a socket to the remote servic
↪e.
TLSv1.0          | Unknown, Reason: Failed to open a socket to the remote servic
↪e.
TLSv1.1          | Unknown, Reason: Failed to open a socket to the remote servic
↪e.
TLSv1.2          | Unknown, Reason: Failed to open a socket to the remote servic
↪e.
TLSv1.3          | Unknown, Reason: Failed to open a socket to the remote servic
↪e.
```

Solution:

Log Method
Details: SSL/TLS: Safe/Secure Renegotiation Support Status
OID:1.3.6.1.4.1.25623.1.0.117757
Version used: 2024-09-27T05:05:23Z

References
url: https://www.gnutls.org/manual/html_node/Safe-renegotiation.html
url: https://wiki.openssl.org/index.php/TLS1.3#Renegotiation
url: https://datatracker.ietf.org/doc/html/rfc5746

Log (CVSS: 0.0)
NVT: SSL/TLS: Version Detection

Summary
Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The remote SSL/TLS service supports the following SSL/TLS protocol version(s): TLSv1.0`

Solution:

Log Method
Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers.
Details: `SSL/TLS: Version Detection`
OID:1.3.6.1.4.1.25623.1.0.105782
Version used: `2024-09-27T05:05:23Z`

[return to 192.168.2.1]

2.2.12 Log 443/tcp

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The service is responding with a 200 HTTP status code to non-existent files/urls
↪. The following pattern is used to work around possible false detections:
-----
 class="splash"
-----
```

Solution:

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, authentication page or redirect instead.

... continues on next page ...

... continued from previous page ...

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: `2023-07-07T05:05:26Z`

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: HTTP Server | Invalid HTTP 00.5 GET request (non-existent HTTP version)
↪to '/'
```

Solution:

Log Method
Details: `HTTP Server Banner Enumeration`
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: `2025-01-31T15:39:24Z`

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

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
```

... continues on next page ...

... continued from previous page ...

↪802067)

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
'Non Weak' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
```

Solution:

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: 2024-09-27T05:05:23Z

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

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing

Summary
The remote web server is not enforcing HTTP Strict Transport Security (HSTS).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote web server is not enforcing HSTS.

... continues on next page ...

... continued from previous page ...

```
HTTP-Banner:
HTTP/1.1 200 OK
Content-Language: en
Content-Type: text/html
Accept-Ranges: bytes
ETag: "***replaced***"
Last-Modified: ***replaced***
Content-Length: ***replaced***
Connection: close
Date: ***replaced***
Server: HTTP Server
```

Solution:
Solution type: Workaround
Enable HSTS or add / configure the required directives correctly following the guides linked in the references.
Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code.
- Apache: Use 'Header always set' instead of 'Header set'.
- nginx: Append the 'always' keyword to each 'add_header' directive.
For different applications or web severs please refer to the related documentation for a similar configuration possibility.

Log Method
Details: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing
OID:1.3.6.1.4.1.25623.1.0.105879
Version used: 2024-02-08T05:05:59Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
url: https://owasp.org/www-project-secure-headers/#http-strict-transport-security-hsts
url: https://tools.ietf.org/html/rfc6797
url: https://securityheaders.io/
url: https://httpd.apache.org/docs/current/mod/mod_headers.html#header
url: https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

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

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

... continues on next page ...

... continued from previous page ...

↪802067)

Summary
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Quality of Detection (QoD): 98%

Vulnerability Detection Result
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

Solution:

Log Method
Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: 2024-09-30T08:38:05Z

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

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

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

... continues on next page ...

... continued from previous page ...

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256

Solution:

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: 2024-09-27T05:05:23Z

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

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate on this port is self-signed.

Quality of Detection (QoD): 98%

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

The certificate of the remote service is self signed.
Certificate details:

fingerprint (SHA-1)	645D99D4857F87CFFB5FFAAD34613E6D97482745
fingerprint (SHA-256)	D19A4E88FB88E985C49DE3E75FC085D55E47CACF8870AC↪429A692B8E7B1497FA
issued by	CN=self-signedkey,O=Sagemcom Ca,C=FR
public key algorithm	RSA
public key size (bits)	2048
serial	00C4BBECECC04303A2
signature algorithm	sha256WithRSAEncryption
subject	CN=self-signedkey,O=Sagemcom Ca,C=FR
subject alternative names (SAN)	None
valid from	2015-10-02 09:55:43 UTC
valid until	2115-09-08 09:55:43 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Self-Signed Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

References
url: http://en.wikipedia.org/wiki/Self-signed_certificate

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

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25↪623.1.0.103692)

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

Quality of Detection (QoD): 98%

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "mynetwork.home".
Certificate details:
fingerprint (SHA-1)             | 645D99D4857F87CFFB5FFAAD34613E6D97482745
fingerprint (SHA-256)           | D19A4E88FB88E985C49DE3E75FC085D55E47CACF8870AC
↪429A692B8E7B1497FA
issued by                       | CN=self-signedkey,O=Sagemcom Ca,C=FR
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 00C4BBECECC04303A2
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=self-signedkey,O=Sagemcom Ca,C=FR
subject alternative names (SAN) | None
valid from                      | 2015-10-02 09:55:43 UTC
valid until                     | 2115-09-08 09:55:43 UTC
```

Solution:

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: 2024-06-14T05:05:48Z

Product Detection Result

Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate Too Long Valid

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The remote server's SSL/TLS certificate expiration date is too far in the future.

Quality of Detection (QoD): 99%

Vulnerability Detection Result

```
The certificate of the remote service is valid for more than 15 years from now a
```

... continues on next page ...

... continued from previous page ...

```
↪nd will expire on 2115-09-08 09:55:43.
Certificate details:
fingerprint (SHA-1)             | 645D99D4857F87CFFB5FFAAD34613E6D97482745
fingerprint (SHA-256)           | D19A4E88FB88E985C49DE3E75FC085D55E47CACF8870AC
↪429A692B8E7B1497FA
issued by                       | CN=self-signedkey,O=Sagemcom Ca,C=FR
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 00C4BBECECC04303A2
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=self-signedkey,O=Sagemcom Ca,C=FR
subject alternative names (SAN) | None
valid from                      | 2015-10-02 09:55:43 UTC
valid until                     | 2115-09-08 09:55:43 UTC
```

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any do not have a reasonable expiration date.

Log Method
Details: `SSL/TLS: Certificate Too Long Valid`
OID:1.3.6.1.4.1.25623.1.0.103958
Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing

Summary
The remote web server is not enforcing HTTP Public Key Pinning (HPKP).
Note: Most major browsers have dropped / deprecated support for this header in 2020.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote web server is not enforcing HPKP.
HTTP-Banner:
HTTP/1.1 200 OK
```

... continues on next page ...

... continued from previous page ...

```
Content-Language: en
Content-Type: text/html
Accept-Ranges: bytes
ETag: "***replaced***"
Last-Modified: ***replaced***
Content-Length: ***replaced***
Connection: close
Date: ***replaced***
Server: HTTP Server
```

Solution:
Solution type: Workaround
Enable HPKP or add / configure the required directives correctly following the guides linked in the references.
Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code.
- Apache: Use 'Header always set' instead of 'Header set'.
- nginx: Append the 'always' keyword to each 'add_header' directive.
For different applications or web severs please refer to the related documentation for a similar configuration possibility.

Log Method
Details: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing
OID:1.3.6.1.4.1.25623.1.0.108247
Version used: 2024-02-08T05:05:59Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-for-http-hpkp
url: https://tools.ietf.org/html/rfc7469
url: https://securityheaders.io/
url: https://httpd.apache.org/docs/current/mod/mod_headers.html#header
url: https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

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

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

Quality of Detection (QoD): 98%

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

... continues on next page ...

... continued from previous page ...

```
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_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.
'Strong' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
No 'Weak' cipher suites accepted by this service via the TLSv1.3 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.3 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.3 protocol.
```

Solution:

Vulnerability Insight
Notes:
- As the VT '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 VT instead.
- SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Log Method
Details: `SSL/TLS: Report Supported Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: `2024-09-27T05:05:23Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: Safe/Secure Renegotiation Support Status

Summary
Checks and reports if a remote SSL/TLS service supports safe/secure renegotiation.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
`Protocol Version | Safe/Secure Renegotiation Support Status`

... continues on next page ...

... continued from previous page ...

```
------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪-----------------------------------
SSLv3            | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.0          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.1          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.2          | Enabled, Note: While the remote service announces the support
↪ of safe/secure renegotiation it still might not support / accept renegotiatio
↪n at all.
TLSv1.3          | Disabled (The TLSv1.3 protocol generally doesn't support rene
↪gotiation so this is always reported as 'Disabled')
```

Solution:

Log Method
Details: SSL/TLS: Safe/Secure Renegotiation Support Status
OID:1.3.6.1.4.1.25623.1.0.117757
Version used: 2024-09-27T05:05:23Z

References
url: https://www.gnutls.org/manual/html_node/Safe-renegotiation.html
url: https://wiki.openssl.org/index.php/TLS1.3#Renegotiation
url: https://datatracker.ietf.org/doc/html/rfc5746

Log (CVSS: 0.0)
NVT: SSL/TLS: Untrusted Certificate Detection

Summary
Checks and reports if a remote SSL/TLS service is using a certificate which is untrusted / the verification against the system wide trust store has failed.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
The remote SSL/TLS server is using the following certificate(s) which failed the ↪ verification against the system wide trust store (serial:issuer):
00C4BBECECC04303A2:CN=self-signedkey,O=Sagemcom Ca,C=FR (Server certificate)

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: SSL/TLS: Untrusted Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.117764
Version used: 2024-09-27T05:05:23Z

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
Expect-CT                         | https://owasp.org/www-project-secure-headers
↪/#expect-ct, Note: This is an upcoming 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
Public-Key-Pins                   | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
```

... continues on next page ...

... continued from previous page ...

```
↪/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
Strict-Transport-Security         | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

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)

... continues on next page ...

... continued from previous page ...

- 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 "mynetwork.home" 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.
The service is responding with a 200 HTTP status code to non-existent files/urls
↪. The following pattern is used to work around possible false detections:
-----
 class="splash"
-----
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; 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:
https://mynetwork.home/
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?/)"
https://mynetwork.home/gui/js
https://mynetwork.home/js/thirdParty
https://mynetwork.home/js/thirdParty/noUiSlider
https://mynetwork.home/js/thirdParty/pikaday
https://mynetwork.home/js/thirdParty/pikaday/css
https://mynetwork.home/js/thirdParty/pikaday/plugins
https://mynetwork.home/layout/css/desktop
The following cgi scripts were excluded from web application scanning because of
↪ the "Regex pattern to exclude cgi scripts" setting of the VT "Web mirroring"
```

... continues on next page ...

... continued from previous page ...

↪(OID: 1.3.6.1.4.1.25623.1.0.10662) for this scan was: "\.(js|css)$"
Syntax : cginame (arguments [default value])
https://mynetwork.home/common-bundle.js (_v [7.2.4])
https://mynetwork.home/gui/js/gui-api.js (_v [7.2.4])
https://mynetwork.home/gui/js/gui-core.js (_v [7.2.4])
https://mynetwork.home/gui/js/jquery-utils.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/IPSubnetCalculator.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/attrchange.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/circle-progress.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/cssua.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/dust-full-0.3.0.min.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/dust-helpers-1.1.1.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/jquery.csv-0.71.min.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/jquery.nouislider.min.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/jquery.sortElements.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/md5.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/modernizr.custom.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css (_v [7.2.4])
https://mynetwork.home/js/thirdParty/noUiSlider/nouislider.min.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/noUiSlider/wNumb.min.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css (_v [7.2.4])
https://mynetwork.home/js/thirdParty/pikaday/css/theme.css (_v [7.2.4])
https://mynetwork.home/js/thirdParty/pikaday/moment.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/pikaday/pikaday.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/pikaday/plugins/pikaday.jquery.js (_v [7.2.
↪4])
https://mynetwork.home/js/thirdParty/raphael.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/typeahead.js (_v [7.2.4])
https://mynetwork.home/js/thirdParty/yepnope.1.5.4-min.js (_v [7.2.4])
https://mynetwork.home/layout/css/desktop/desktop.css (_v [7.2.4])
https://mynetwork.home/main-bundle.js (_v [7.2.4])
https://mynetwork.home/system-csp-production.js (_v [7.2.4])

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: 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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: HTTP Server`

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`

Log (CVSS: 0.0)
NVT: SSL/TLS: Version Detection

Summary
Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The remote SSL/TLS service supports the following SSL/TLS protocol version(s):`
`TLSv1.2`
`TLSv1.3`

Solution:

Log Method
Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers.
Details: `SSL/TLS: Version Detection`
OID:1.3.6.1.4.1.25623.1.0.105782
Version used: `2024-09-27T05:05:23Z`

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.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)             | 645D99D4857F87CFFB5FFAAD34613E6D97482745
fingerprint (SHA-256)           | D19A4E88FB88E985C49DE3E75FC085D55E47CACF8870AC
↪429A692B8E7B1497FA
issued by                       | CN=self-signedkey,O=Sagemcom Ca,C=FR
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 00C4BBECECC04303A2
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=self-signedkey,O=Sagemcom Ca,C=FR
subject alternative names (SAN) | None
valid from                      | 2015-10-02 09:55:43 UTC
valid until                     | 2115-09-08 09:55:43 UTC
```

Solution:

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
A TLScustom server answered on this port
```

Solution:

. . . continues on next page . . .

... continued from previous page ...

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: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

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

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`

[return to 192.168.2.1]

2.2.13 Log 10080/tcp

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.

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The host returns a 30x (e.g. 301) error code when a non-existent file is request ↪ed. Some HTTP-related checks have been disabled.`

Solution:

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, authentication page or redirect 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: `2023-07-07T05:05:26Z`

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: HTTP Server`

Solution:

Log Method

... continues on next page ...

... continued from previous page ...

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

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: HTTP Server | Invalid HTTP 00.5 GET request (non-existent HTTP version)
↪to '/'
```

Solution:

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

... continues on next page ...

... continued from previous page ...

```
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

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

... continues on next page ...

... continued from previous page ...

```
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 "mynetwork.home" 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 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://mynetwork.home:10080/
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
```

Solution:

Log Method

... continues on next page ...

... continued from previous page ...

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: 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

[return to 192.168.2.1]

2.2.14 Log 80/tcp

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.

Quality of Detection (QoD): 80%

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
The service is responding with a 200 HTTP status code to non-existent files/urls
↪. The following pattern is used to work around possible false detections:
-----
 class="splash"
-----
```

Solution:

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, authentication page or redirect 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: `2023-07-07T05:05:26Z`

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote HTTP Server banner is:
Server: HTTP Server
```

Solution:

Log Method

... continues on next page ...

... continued from previous page ...

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

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: HTTP Server | Invalid HTTP 00.5 GET request (non-existent HTTP version)
↪to '/'
```

Solution:

Log Method
Details: HTTP Server Banner Enumeration
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: 2025-01-31T15:39:24Z

Log (CVSS: 0.0)
NVT: SSL/TLS: HPKP / HSTS / Expect-CT Headers sent via plain HTTP

Summary
This script checks if the remote HTTP server is sending a HPKP, HSTS and/or Expect-CT header via plain HTTP.
Note: Most major browsers have dropped / deprecated support for this header in 2020.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote HTTP server is sending HPKP, HSTS and/or Expect-CT headers via plain
↪HTTP.
HSTS-Header:
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
```

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: Workaround
Configure the remote host to only send HPKP, HSTS and Expect-CT headers via HTTPS. Sending those headers via plain HTTP doesn't comply with the referenced RFCs.

Log Method
Details: SSL/TLS: HPKP / HSTS / Expect-CT Headers sent via plain HTTP
OID:1.3.6.1.4.1.25623.1.0.108248
Version used: 2023-07-25T05:05:58Z

References
url: https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-for-http-hpkp
url: https://owasp.org/www-project-secure-headers/#http-strict-transport-security-hsts
url: https://owasp.org/www-project-secure-headers/#expect-ct
url: https://tools.ietf.org/html/rfc6797
url: https://tools.ietf.org/html/rfc7469
url: https://securityheaders.io/
url: http://httpwg.org/http-extensions/expect-ct.html#http-request-type

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

Header Name	Header Value
X-Content-Type-Options	nosniff
X-Frame-Options	DENY
X-XSS-Protection	1; mode=block

Missing Headers	More Information
Content-Security-Policy	https://owasp.org/www-project-secure-headers/#content-security-policy

... continues on next page ...

... continued from previous page ...

```
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-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
```

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

... continues on next page ...

... continued from previous page ...

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 "mynetwork.home" 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.
The service is responding with a 200 HTTP status code to non-existent files/urls
↪. The following pattern is used to work around possible false detections:
-----
 class="splash"
-----
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; 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://mynetwork.home/
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://mynetwork.home/gui/js
http://mynetwork.home/js/thirdParty
http://mynetwork.home/js/thirdParty/noUiSlider
```

... continues on next page ...

... continued from previous page ...

```
http://mynetwork.home/js/thirdParty/pikaday
http://mynetwork.home/js/thirdParty/pikaday/css
http://mynetwork.home/js/thirdParty/pikaday/plugins
http://mynetwork.home/layout/css/desktop
The following cgi scripts were excluded from web application scanning because of
↪ the "Regex pattern to exclude cgi scripts" setting of the VT "Web mirroring"
↪(OID: 1.3.6.1.4.1.25623.1.0.10662) for this scan was: "\.(js|css)$"
Syntax : cginame (arguments [default value])
http://mynetwork.home/common-bundle.js (_v [7.2.4] )
http://mynetwork.home/gui/js/gui-api.js (_v [7.2.4] )
http://mynetwork.home/gui/js/gui-core.js (_v [7.2.4] )
http://mynetwork.home/gui/js/jquery-utils.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/IPSubnetCalculator.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/attrchange.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/circle-progress.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/cssua.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/dust-full-0.3.0.min.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/dust-helpers-1.1.1.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/jquery-1.8.3.min.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/jquery.csv-0.71.min.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/jquery.nouislider.min.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/jquery.sortElements.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/md5.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/modernizr.custom.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/noUiSlider/nouislider.css (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/noUiSlider/nouislider.min.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/noUiSlider/wNumb.min.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/pikaday/css/pikaday.css (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/pikaday/css/theme.css (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/pikaday/moment.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/pikaday/pikaday.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/pikaday/plugins/pikaday.jquery.js (_v [7.2.4
↪] )
http://mynetwork.home/js/thirdParty/raphael.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/typeahead.js (_v [7.2.4] )
http://mynetwork.home/js/thirdParty/yepnope.1.5.4-min.js (_v [7.2.4] )
http://mynetwork.home/layout/css/desktop/desktop.css (_v [7.2.4] )
http://mynetwork.home/main-bundle.js (_v [7.2.4] )
http://mynetwork.home/system-csp-production.js (_v [7.2.4] )
```

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`

... continues on next page ...

... continued from previous page ...

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

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`

[return to 192.168.2.1]

2.2.15 Log 9000/tcp

Log (CVSS: 0.0)
NVT: UPnP Detection (TCP)

Summary
TCP based detection of the UPnP protocol.
The script sends a HTTP request to URLs for the root description XML, either based on previously detected location or a list of known possible locations.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The remote Host exposes an UPnP root device XML on port 9000/tcp.`
`The XML can be found at the location:`

... continues on next page ...

... continued from previous page ...

http://mynetwork.home:9000/rss/Starter_desc.xml

Solution:

Log Method
Details: UPnP Detection (TCP)
OID:1.3.6.1.4.1.25623.1.0.170204
Version used: 2024-09-06T15:39:29Z

References
url: https://openconnectivity.org/foundation/faq/upnp-faq/

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote HTTP Server banner is:
Server: Linux/2.x.x, UPnP/1.0, pvConnect UPnP SDK/1.0, Twonky UPnP SDK/1.1

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

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):

... continues on next page ...

... continued from previous page ...

```
Server banner                                                                 | Enu
↪meration technique
------------------------------------------------------------------------------
↪-------------------------------------------------------------
Server: Linux/2.x.x, UPnP/1.0, pvConnect UPnP SDK/1.0, Twonky UPnP SDK/1.1 | Inv
↪alid HTTP 00.5 GET request (non-existent HTTP version) to '/'
```

Solution:

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

... continues on next page ...

... continued from previous page ...

```
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

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

... continues on next page ...

... continued from previous page ...

- 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 "mynetwork.home" 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 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://mynetwork.home:9000/
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
```

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: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

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

[return to 192.168.2.1]

2.3 192.168.2.66

Host scan start Thu Mar 6 04:55:41 2025 UTC
Host scan end Thu Mar 6 06:45:22 2025 UTC

Service (Port)	Threat Level
443/tcp	Medium
general/icmp	Low
general/tcp	Low
2020/tcp	Log
443/tcp	Log
8800/tcp	Log
general/CPE-T	Log
554/tcp	Log
10443/tcp	Log
general/tcp	Log

2.3.1 Medium 443/tcp

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

Summary
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

Quality of Detection (QoD): 80%

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:00D1167079029DDD0D:O=TPRI,CN=TPRI-DEVICE,ST=CA,C=US (Server certificate
↪)

Impact
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

Solution:
Solution type: Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

Vulnerability Insight
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

Vulnerability Detection Method
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

References
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

[return to 192.168.2.66]

2.3.2 Low general/icmp

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

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0

... continues on next page ...

... continued from previous page ...

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 192.168.2.66]

2.3.3 Low general/tcp

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

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 131325079
Packet 2: 131325196
```

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 192.168.2.66]

2.3.4 Log 2020/tcp

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This VT consolidates and reports the information collected by the following VTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)
If you know any of the information reported here, please send the full output to the referenced community forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Nmap service detection (unknown) result for this port: tcpwrapped`

Solution:

Log Method
Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `2023-06-22T10:34:15Z`

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

[return to 192.168.2.66]

2.3.5 Log 443/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

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

Solution:

Vulnerability Insight
. . . continues on next page . . .

... continued from previous page ...

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: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

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

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: SSL/TLS: Version Detection

Summary
Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The remote SSL/TLS service supports the following SSL/TLS protocol version(s): TLSv1.2`

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers.
Details: SSL/TLS: Version Detection
OID:1.3.6.1.4.1.25623.1.0.105782
Version used: 2024-09-27T05:05:23Z

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.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)             | 7BA8899B6211B5479A6D07AA92BE0B12BBD5C28F
fingerprint (SHA-256)           | C3F14B8C36EE916031CA4FE49582BD3B8C9467095A3A4C
↪AC0045036FA8E62412
issued by                       | O=TPRI,CN=TPRI-DEVICE,ST=CA,C=US
public key algorithm            | RSA
public key size (bits)          | 1024
serial                          | 00D1167079029DDD0D
signature algorithm             | sha256WithRSAEncryption
subject                         | O=TPRI,CN=TPRI-DEVICE,ST=CA,C=US
subject alternative names (SAN) | None
valid from                      | 2023-12-07 07:48:57 UTC
valid until                     | 2073-11-24 07:48:57 UTC
```

Solution:

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate on this port is self-signed.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
The certificate of the remote service is self signed.
Certificate details:

fingerprint (SHA-1)	7BA8899B6211B5479A6D07AA92BE0B12BBD5C28F
fingerprint (SHA-256)	C3F14B8C36EE916031CA4FE49582BD3B8C9467095A3A4C ↪AC0045036FA8E62412
issued by	O=TPRI,CN=TPRI-DEVICE,ST=CA,C=US
public key algorithm	RSA
public key size (bits)	1024
serial	00D1167079029DDD0D
signature algorithm	sha256WithRSAEncryption
subject	O=TPRI,CN=TPRI-DEVICE,ST=CA,C=US
subject alternative names (SAN)	None
valid from	2023-12-07 07:48:57 UTC
valid until	2073-11-24 07:48:57 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Self-Signed Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

References
url: http://en.wikipedia.org/wiki/Self-signed_certificate

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate Too Long Valid

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The remote server's SSL/TLS certificate expiration date is too far in the future.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
The certificate of the remote service is valid for more than 15 years from now a
↪nd will expire on 2073-11-24 07:48:57.
Certificate details:

fingerprint (SHA-1)	7BA8899B6211B5479A6D07AA92BE0B12BBD5C28F
fingerprint (SHA-256)	C3F14B8C36EE916031CA4FE49582BD3B8C9467095A3A4C ↪AC0045036FA8E62412
issued by	O=TPRI,CN=TPRI-DEVICE,ST=CA,C=US
public key algorithm	RSA
public key size (bits)	1024
serial	00D1167079029DDD0D
signature algorithm	sha256WithRSAEncryption
subject	O=TPRI,CN=TPRI-DEVICE,ST=CA,C=US
subject alternative names (SAN)	None
valid from	2023-12-07 07:48:57 UTC
valid until	2073-11-24 07:48:57 UTC

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any do not have a reasonable expiration date.

Log Method
Details: SSL/TLS: Certificate Too Long Valid
OID:1.3.6.1.4.1.25623.1.0.103958
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing

Summary
The remote web server is not enforcing HTTP Public Key Pinning (HPKP).
Note: Most major browsers have dropped / deprecated support for this header in 2020.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The remote web server is not enforcing HPKP.
HTTP-Banner:
HTTP/1.1 404 Not Found
Connection: close
Cache-Control: no-cache
```

Solution:
Solution type: Workaround
Enable HPKP or add / configure the required directives correctly following the guides linked in the references.
Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code.
- Apache: Use 'Header always set' instead of 'Header set'.
- nginx: Append the 'always' keyword to each 'add_header' directive.
For different applications or web severs please refer to the related documentation for a similar configuration possibility.

Log Method
Details: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing
OID:1.3.6.1.4.1.25623.1.0.108247
Version used: 2024-02-08T05:05:59Z

References
```
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-
↪for-http-hpkp
url: https://tools.ietf.org/html/rfc7469
url: https://securityheaders.io/
url: https://httpd.apache.org/docs/current/mod/mod_headers.html#header
url: https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header
```

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing

Summary
The remote web server is not enforcing HTTP Strict Transport Security (HSTS).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The remote web server is not enforcing HSTS.
HTTP-Banner:
HTTP/1.1 404 Not Found
Connection: close
Cache-Control: no-cache
```

Solution:
Solution type: Workaround
Enable HSTS or add / configure the required directives correctly following the guides linked in the references.
Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code.
- Apache: Use 'Header always set' instead of 'Header set'.
- nginx: Append the 'always' keyword to each 'add_header' directive.
For different applications or web severs please refer to the related documentation for a similar configuration possibility.

Log Method
Details: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing
OID:1.3.6.1.4.1.25623.1.0.105879
Version used: 2024-02-08T05:05:59Z

References
```
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transpor
↪t_Security_Cheat_Sheet.html
url: https://owasp.org/www-project-secure-headers/#http-strict-transport-securit
↪y-hsts
url: https://tools.ietf.org/html/rfc6797
url: https://securityheaders.io/
url: https://httpd.apache.org/docs/current/mod/mod_headers.html#header
url: https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header
```

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

. . . continues on next page . . .

... continued from previous page ...

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

Quality of Detection (QoD): 98%

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

Solution:

Log Method
Details: `SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing`
OID:1.3.6.1.4.1.25623.1.0.105092
Version used: `2024-09-27T05:05:23Z`

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

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

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
`'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:`
`TLS_RSA_WITH_AES_128_CBC_SHA256`
`TLS_RSA_WITH_AES_128_GCM_SHA256`
`TLS_RSA_WITH_AES_256_CBC_SHA256`
`TLS_RSA_WITH_AES_256_GCM_SHA384`

Solution:

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`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.902816
Version used: 2024-09-27T05:05:23Z

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

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

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

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Solution:

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: 2024-09-27T05:05:23Z

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

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

... continues on next page ...

... continued from previous page ...

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
Expect-CT                         | https://owasp.org/www-project-secure-headers
↪/#expect-ct, Note: This is an upcoming 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
Public-Key-Pins                   | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
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
```

... continues on next page ...

... continued from previous page ...

```
↪rted only in newer browsers like e.g. Firefox 90
Strict-Transport-Security         | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

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: SSL/TLS: Report Supported Cipher Suites

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
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_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_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.
```

Solution:

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Notes:
- As the VT '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 VT instead.
- SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Log Method
Details: `SSL/TLS: Report Supported Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: `2024-09-27T05:05:23Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: Safe/Secure Renegotiation Support Status

Summary
Checks and reports if a remote SSL/TLS service supports safe/secure renegotiation.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
Protocol Version | Safe/Secure Renegotiation Support Status
------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪-----------------------------------
SSLv3            | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.0          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.1          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.2          | Enabled, Note: While the remote service announces the support
↪ of safe/secure renegotiation it still might not support / accept renegotiatio
↪n at all.
TLSv1.3          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
```

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: SSL/TLS: Safe/Secure Renegotiation Support Status
OID:1.3.6.1.4.1.25623.1.0.117757
Version used: 2024-09-27T05:05:23Z

References
url: https://www.gnutls.org/manual/html_node/Safe-renegotiation.html
url: https://wiki.openssl.org/index.php/TLS1.3#Renegotiation
url: https://datatracker.ietf.org/doc/html/rfc5746

Log (CVSS: 0.0)
NVT: SSL/TLS: Untrusted Certificate Detection

Summary
Checks and reports if a remote SSL/TLS service is using a certificate which is untrusted / the verification against the system wide trust store has failed.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
The remote SSL/TLS server is using the following certificate(s) which failed the
↪ verification against the system wide trust store (serial:issuer):
00D1167079029DDD0D:O=TPRI,CN=TPRI-DEVICE,ST=CA,C=US (Server certificate)

Solution:

Log Method
Details: SSL/TLS: Untrusted Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.117764
Version used: 2024-09-27T05:05:23Z

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

... continues on next page ...

... continued from previous page ...

- 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 "192.168.2.66" 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 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:
https://192.168.2.66/
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
```

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`

[return to 192.168.2.66]

2.3.6 Log 8800/tcp

Log (CVSS: 0.0)
NVT: Services

Summary

... continues on next page ...

... continued from previous page ...

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: 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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The remote web server is very slow - it took 206 seconds (Maximum response time
↪configured in 'Response Time / No 404 Error Code Check' (OID: 1.3.6.1.4.1.2562
↪3.1.0.10386) preferences: 60 seconds) to execute the plugin no404.nasl (it usu
↪ally 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.
```

Solution:

Vulnerability Insight
This web server might show the following issues:

... continues on next page ...

... continued from previous page ...

- 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, authentication page or redirect 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: `2023-07-07T05:05:26Z`

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 "192.168.2.66" 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 web application scanning is launched aga
↪inst it. Reason(s):
-----
 - The remote web server is very slow - it took 206 seconds (Maximum response ti
↪me configured in 'Response Time / No 404 Error Code Check' (OID: 1.3.6.1.4.1.2
↪5623.1.0.10386) preferences: 60 seconds) to execute the plugin no404.nasl (it
```

... continues on next page ...

... continued from previous page ...

```
↪usually 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/1.0.
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://192.168.2.66:8800/
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
```

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

[return to 192.168.2.66]

2.3.7 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:

... continues on next page ...

... continued from previous page ...

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
192.168.2.66|cpe:/a:ietf:transport_layer_security:1.2
192.168.2.66|cpe:/o:linux:kernel

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

[return to 192.168.2.66]

2.3.8 Log 554/tcp

Log (CVSS: 0.0)
NVT: Service Detection with 'SIP' Request

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
A streaming server seems to be running on this port.

Solution:

Vulnerability Insight
This plugin is a complement of the plugin 'Services' (OID: 1.3.6.1.4.1.25623.1.0.10330). It sends a 'SIP OPTIONS' request to the remaining unknown services and tries to identify them.

Log Method
Details: Service Detection with 'SIP' Request
OID:1.3.6.1.4.1.25623.1.0.108203

... continues on next page ...

... continued from previous page ...

Version used: 2023-06-14T05:05:19Z

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

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
All RTSP Header for 'OPTIONS *' method:
RTSP/1.0 200 OK
CSeq: 0
Date: Thu, Mar 06 2025 04:57:36 GMT
Public: OPTIONS, DESCRIBE, SETUP, TEARDOWN, PLAY, PAUSE, GET_PARAMETER, SET_PARA
↪METER
```

Solution:

Log Method
Details: RTSP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10762
Version used: 2023-08-01T13:29:10Z

[return to 192.168.2.66]

2.3.9 Log 10443/tcp

Log (CVSS: 0.0)
NVT: SSL/TLS: Version Detection

Summary
Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote SSL/TLS service supports the following SSL/TLS protocol version(s):
TLSv1.2
```

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers.
Details: `SSL/TLS: Version Detection`
OID:1.3.6.1.4.1.25623.1.0.105782
Version used: `2024-09-27T05:05:23Z`

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This VT consolidates and reports the information collected by the following VTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)
If you know any of the information reported here, please send the full output to the referenced community forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Nmap service detection (unknown) result for this port: ssl|unknown`

Solution:

Log Method
Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `2023-06-22T10:34:15Z`

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

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

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

... continues on next page ...

... continued from previous page ...

Summary
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Quality of Detection (QoD): 98%

Vulnerability Detection Result
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.2 protocol:
TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA

Solution:

Log Method
Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: 2024-09-30T08:38:05Z

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

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

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

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA

Solution:

... continues on next page ...

... continued from previous page ...

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: 2024-09-27T05:05:23Z

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

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

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

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA

Solution:

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: 2024-09-27T05:05:23Z

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

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

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
```
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_ECDHE_PSK_WITH_AES_128_CBC_SHA
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.
```

Solution:

Vulnerability Insight
Notes:
- As the VT '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 VT instead.
- SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Log Method
Details: SSL/TLS: Report Supported Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Safe/Secure Renegotiation Support Status

Summary
Checks and reports if a remote SSL/TLS service supports safe/secure renegotiation.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
```
Protocol Version | Safe/Secure Renegotiation Support Status
------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪-------------------------------------
SSLv3            | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
```

... continues on next page ...

... continued from previous page ...

```
↪pting this SSL/TLS protocol version).
TLSv1.0          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.1          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.2          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.3          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
```

Solution:

Log Method
Details: SSL/TLS: Safe/Secure Renegotiation Support Status
OID:1.3.6.1.4.1.25623.1.0.117757
Version used: 2024-09-27T05:05:23Z

References
url: https://www.gnutls.org/manual/html_node/Safe-renegotiation.html
url: https://wiki.openssl.org/index.php/TLS1.3#Renegotiation
url: https://datatracker.ietf.org/doc/html/rfc5746

[return to 192.168.2.66]

2.3.10 Log general/tcp

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.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
The following additional but not resolvable hostnames were detected:
TPRI-DEVICE

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: SSL/TLS: Hostname discovery from server certificate
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: 2021-11-22T15:32:39Z

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:           Linux Kernel
CPE:          cpe:/o:linux:kernel
Found by VT:  1.3.6.1.4.1.25623.1.0.102002 (Operating System (OS) Detection (ICM
↪P))
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
```

Solution:

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

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

Log (CVSS: 0.0)
NVT: IP Forwarding Enabled - Active Check

Summary
Checks if the remote host has IP forwarding enabled.

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 70%

Vulnerability Detection Result
`It was possible to route an ICMP packet through the target host and received an ↪answer which means IP forwarding is enabled.`

Solution:

Log Method
Sends a crafted Local Link Layer (LLL) frame and checks the response.
Details: `IP Forwarding Enabled - Active Check`
OID:1.3.6.1.4.1.25623.1.0.147205
Version used: `2021-12-03T08:27:06Z`

References
`cve: CVE-1999-0511`

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 (192.168.2.108) to target (192.168.2.66):
192.168.2.108
192.168.2.66
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`

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 192.168.2.66:`
`Hostname|Source`
`192.168.2.66|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`

[return to 192.168.2.66]

2.4 192.168.2.107

Host scan start Thu Mar 6 02:25:27 2025 UTC
Host scan end Thu Mar 6 04:48:44 2025 UTC

Service (Port)	Threat Level
general/tcp	Low
general/icmp	Low
general/CPE-T	Log
9200/tcp	Log
general/tcp	Log

2.4.1 Low general/tcp

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

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

Quality of Detection (QoD): 80%

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 2274485180
Packet 2: 2274486300

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 192.168.2.107]

2.4.2 Low general/icmp

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

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

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

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

Solution:
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 192.168.2.107]

2.4.3 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
192.168.2.107|cpe:/a:elastic:elasticsearch:8.17.2
192.168.2.107|cpe:/a:elastic:logstash:8.17.2
192.168.2.107|cpe:/a:elasticsearch:elasticsearch:8.17.2
192.168.2.107|cpe:/a:elasticsearch:logstash:8.17.2
192.168.2.107|cpe:/o:linux:kernel

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

[return to 192.168.2.107]

2.4.4 Log 9200/tcp

Log (CVSS: 0.0)
NVT: Elastic Elasticsearch and Logstash Detection (HTTP)

Summary
HTTP based detection of Elastic Elasticsearch.
Note: Once a Elasticsearch service was detected it is assumed that Logstash is installed in the same version (ELK Stack).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Detected Elastic Elasticsearch

... continues on next page ...

... continued from previous page ...

```
Version:       8.17.2
Location:      /
CPE:           cpe:/a:elastic:elasticsearch:8.17.2
Concluded from version/product identification result:
number" : "8.17.2",
Extra information:
Collected information (truncated) from http://192.168.2.107:9200/_cat/indices?v
↪:
health status index
↪ uuid                   pri rep docs.count docs.deleted store.size pri.store.s
↪ize dataset.size
green  open   .internal.alerts-transform.health.alerts-default-000001
↪ SwZjTE-SS0i1Jkj7pHEW1w   1   0          0            0       249b           2
↪49b         249b
yellow open   index.cfm
↪ vJxRBTc6T96ht3Labfzn5g   1   1          0            0       249b           2
↪49b         249b
green  open   .internal.alerts-ml.anomaly-detection.alerts-default-000001
↪ l-zodJ-eSIuHGsLNg3FjgQ   1   0          0            0       249b           2
↪49b         249b
yellow open   index.htm
↪ -rjgFz30Qg-bTKA1W0ls5A   1   1          0            0       249b           2
↪49b         249b
green  open   .internal.alerts-observability.slo.alerts-default-000001
↪ TZqoswdjTZmrcfHDQ_ho2Q   1   0          0
Detected Elastic Logstash
Version:       8.17.2
Location:      /
CPE:           cpe:/a:elastic:logstash:8.17.2
Concluded from version/product identification result:
Existence of Elasticsearch service, the actual version of the Logstash service m
↪ight differ.
```

Solution:

Log Method
Details: Elastic Elasticsearch and Logstash Detection (HTTP)
OID:1.3.6.1.4.1.25623.1.0.105031
Version used: 2024-04-30T05:05:26Z

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

Summary
All known security headers are being checked on the remote web server.

... continues on next page ...

... continued from previous page ...

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
↪/#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
```

... continues on next page ...

... continued from previous page ...

```
↪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 "192.168.2.107" 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 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
```

... continues on next page ...

... continued from previous page ...

```
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
http://192.168.2.107:9200/
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
```

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: 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`

[return to 192.168.2.107]

2.4.5 Log general/tcp

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:           Linux Kernel
CPE:          cpe:/o:linux:kernel
Found by VT:  1.3.6.1.4.1.25623.1.0.102002 (Operating System (OS) Detection (ICM
↪P))
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
```

Solution:

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

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

Log (CVSS: 0.0)
NVT: IP Forwarding Enabled - Active Check

Summary
Checks if the remote host has IP forwarding enabled.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
```
It was possible to route an ICMP packet through the target host and received an
↪answer which means IP forwarding is enabled.
```

Solution:

. . . continues on next page . . .

... continued from previous page ...

Log Method
Sends a crafted Local Link Layer (LLL) frame and checks the response.
Details: `IP Forwarding Enabled - Active Check`
OID:1.3.6.1.4.1.25623.1.0.147205
Version used: `2021-12-03T08:27:06Z`

References
`cve: CVE-1999-0511`

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 (192.168.2.108) to target (192.168.2.107):
192.168.2.108
192.168.2.107
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`

Log (CVSS: 0.0)
NVT: Hostname Determination Reporting

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

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Hostname determination for IP 192.168.2.107:
Hostname|Source
192.168.2.107|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

[return to 192.168.2.107]

2.5 192.168.2.98

Host scan start Thu Mar 6 03:44:57 2025 UTC
Host scan end Thu Mar 6 05:24:47 2025 UTC

Service (Port)	Threat Level
general/tcp	Low
general/tcp	Log
7680/tcp	Log

2.5.1 Low general/tcp

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

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 305911715
Packet 2: 305912890

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

... continues on next page ...

... continued from previous page ...

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 192.168.2.98]

2.5.2 Log general/tcp

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%

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Network route from scanner (192.168.2.108) to target (192.168.2.98):
192.168.2.108
192.168.2.98
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

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
No Best matching OS identified. Please see the VT 'Unknown OS and Service Banner Reporting' (OID: 1.3.6.1.4.1.25623.1.0.108441) for possible ways to identify this OS.

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

... continues on next page ...

... continued from previous page ...

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

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 192.168.2.98:
Hostname|Source
192.168.2.98|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

[return to 192.168.2.98]

2.5.3 Log 7680/tcp

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This VT consolidates and reports the information collected by the following VTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)
If you know any of the information reported here, please send the full output to the referenced community forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Nmap service detection (unknown) result for this port: pando-pub

... continues on next page ...

... continued from previous page ...

```
This is a guess. A confident identification of the service was not possible.
Hint: If you're running a recent nmap version try to run nmap with the following
↪ command: 'nmap -sV -Pn -p 7680 192.168.2.98' and submit a possible collected
↪fingerprint to the nmap database.
```

Solution:

Log Method
Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `2023-06-22T10:34:15Z`

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

[return to 192.168.2.98]

2.6 192.168.2.106

Host scan start Thu Mar 6 02:25:27 2025 UTC
Host scan end Thu Mar 6 05:00:01 2025 UTC

Service (Port)	Threat Level
general/icmp	Low
general/tcp	Low
general/tcp	Log
443/tcp	Log
80/tcp	Log
general/CPE-T	Log

2.6.1 Low general/icmp

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

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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

... continues on next page ...

... continued from previous page ...

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 192.168.2.106]

2.6.2 Low general/tcp

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

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1818462455
Packet 2: 1818463515
```

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 192.168.2.106]

2.6.3 Log general/tcp

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:           Greenbone OS (GOS) 22.04.27
Version:      22.04.27
CPE:          cpe:/o:greenbone:greenbone_os:22.04.27
Found by VT:  1.3.6.1.4.1.25623.1.0.103220 (Greenbone Security Manager (GSM) / G
↪reenbone OS (GOS) Detection Consolidation)
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:  1.3.6.1.4.1.25623.1.0.103841 (Greenbone Security Assistant (GSA) D
↪etection (HTTP))
```

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: nginx Detection Consolidation

Summary
Consolidation of nginx detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

```
Detected nginx
Version:       unknown
Location:      443/tcp
CPE:           cpe:/a:nginx:nginx
Concluded from version/product identification result:
Server: nginx
Detected nginx
Version:       unknown
Location:      80/tcp
CPE:           cpe:/a:nginx:nginx
Concluded from version/product identification result:
Server: nginx
<hr><center>nginx</center>
Concluded from version/product identification location:
http://192.168.2.106/
```

Solution:

Log Method
Details: `nginx Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.113787
Version used: `2022-02-03T09:26:44Z`

References
`url: https://www.nginx.com/`

Log (CVSS: 0.0)
NVT: IP Forwarding Enabled - Active Check

Summary
Checks if the remote host has IP forwarding enabled.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
`It was possible to route an ICMP packet through the target host and received an ↪answer which means IP forwarding is enabled.`

Solution:

Log Method
Sends a crafted Local Link Layer (LLL) frame and checks the response.
Details: `IP Forwarding Enabled - Active Check`
OID:1.3.6.1.4.1.25623.1.0.147205

... continues on next page ...

... continued from previous page ...

Version used: 2021-12-03T08:27:06Z

References
cve: CVE-1999-0511

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 (192.168.2.108) to target (192.168.2.106):
192.168.2.108
192.168.2.106
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

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 192.168.2.106:
Hostname|Source

... continues on next page ...

... continued from previous page ...

192.168.2.106|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: 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.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
The following additional and resolvable hostnames pointing to a different host i
↪p were detected:
gsm.gbuser.net

Solution:

Log Method
Details: SSL/TLS: Hostname discovery from server certificate
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: 2021-11-22T15:32:39Z

Log (CVSS: 0.0)
NVT: Greenbone Security Manager (GSM) / Greenbone OS (GOS) Detection Consolidation

Summary
Consolidation of Greenbone Security Manager (GSM) / Greenbone OS (GOS) detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Detected Greenbone OS (GOS)
Version: 22.04.27
Location: /
CPE: cpe:/o:greenbone:greenbone_os:22.04.27

... continues on next page ...

... continued from previous page ...

```
Detected Greenbone Security Manager (GSM) TRIAL
Location:       /
CPE:            cpe:/a:greenbone:gsm_trial
Detection methods:
- HTTP(s) on port 443/tcp
  Concluded from version/product identification result: vendorVersion: 'Greenbon
↪e OS 22.04.27',<newline>vendorLabel: 'gsm-trial_label.svg',
  Concluded from version/product identification location: https://192.168.2.106/
↪login and https://192.168.2.106/config.js
```

Solution:

Log Method
Details: Greenbone Security Manager (GSM) / Greenbone OS (GOS) Detection Consolidation
OID:1.3.6.1.4.1.25623.1.0.103220
Version used: 2022-08-11T10:10:35Z

[return to 192.168.2.106]

2.6.4 Log 443/tcp

Log (CVSS: 0.0)
NVT: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

Summary
This routine identifies services supporting the following extensions to TLS:
- Application-Layer Protocol Negotiation (ALPN)
- Next Protocol Negotiation (NPN).
Based on the availability of this extensions the supported Network Protocols by this service are gathered and reported.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote service advertises support for the following Network Protocol(s) via
↪the NPN extension:
SSL/TLS Protocol:Network Protocol
TLSv1.2:HTTP/1.1
TLSv1.2:HTTP/2
The remote service advertises support for the following Network Protocol(s) via
↪the ALPN extension:
SSL/TLS Protocol:Network Protocol
TLSv1.2:HTTP/1.1
TLSv1.2:HTTP/2
```

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
OID:1.3.6.1.4.1.25623.1.0.108099
Version used: 2024-09-27T05:05:23Z

References
url: https://tools.ietf.org/html/rfc7301
url: https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote HTTP Server banner is:
Server: nginx

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

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)

... continues on next page ...

... continued from previous page ...

- 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 "192.168.2.106" 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.
The service is responding with a 200 HTTP status code to non-existent files/urls
↪. The following pattern is used to work around possible false detections:
-----
Greenbone Enterprise Appliance
-----
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; 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:
https://192.168.2.106/
https://192.168.2.106/assets
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?/)"
https://192.168.2.106/img
```

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

... continues on next page ...

... continued from previous page ...

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

Log (CVSS: 0.0)
NVT: robot.txt / robots.txt exists on the Web Server (HTTP)

Summary
Web Servers can use a file called /robot(s).txt to ask search engines to ignore certain files and directories. By nature this file can not be used to protect private files from public read access.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The file 'https://192.168.2.106/robots.txt' contains the following:
User-agent: *
Disallow: /
```

Solution:
Solution type: Mitigation
Review the content of the /robot(s).txt file and consider removing the files from the server or protect them in other ways in case you actually intended non-public availability.

Vulnerability Insight
Any serious web search engine will honor the /robot(s).txt file and not scan the files and directories listed there.
Any entries listed in this file are not even hidden anymore.

Log Method
Details: robot.txt / robots.txt exists on the Web Server (HTTP)
OID:1.3.6.1.4.1.25623.1.0.10302
Version used: 2024-02-26T14:36:40Z

References
url: https://www.robotstxt.org/
url: https://www.robotstxt.org/norobots-rfc.txt

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

... continues on next page ...

... continued from previous page ...

Summary
The SSL/TLS certificate on this port is self-signed.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
The certificate of the remote service is self signed.
Certificate details:
fingerprint (SHA-1)              | D3C255C6D78958DDE7DAD760D290E990E4C02A08
fingerprint (SHA-256)            | 2033B1DCFC10EC3189B15C5E6CE7791BB257D53783A03B
↪55CBD9C612393B4860
issued by                        | C=DE,ST=Niedersachsen,L=Osnabrueck,O=Greenbone
↪ AG Customer,OU=Vulnerability Management Team,CN=gsm.gbuser.net
public key algorithm             | RSA
public key size (bits)           | 3072
serial                           | 0CC5B263F56BB28519DD46EB06981D5225624BD1
signature algorithm              | sha256WithRSAEncryption
subject                          | C=DE,ST=Niedersachsen,L=Osnabrueck,O=Greenbone
↪ AG Customer,OU=Vulnerability Management Team,CN=gsm.gbuser.net
subject alternative names (SAN)  | gsm.gbuser.net
valid from                       | 2025-02-07 07:40:09 UTC
valid until                      | 2027-02-07 07:40:09 UTC
```

Solution:

Log Method
Details: SSL/TLS: Certificate - Self-Signed Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

References
url: http://en.wikipedia.org/wiki/Self-signed_certificate

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing

Summary
The remote web server is not enforcing HTTP Public Key Pinning (HPKP).

... continues on next page ...

... continued from previous page ...

Note: Most major browsers have dropped / deprecated support for this header in 2020.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote web server is not enforcing HPKP.
HTTP-Banner:
HTTP/1.1 200 OK
Server: nginx
Date: ***replaced***
Content-Type: text/html; charset=utf-8
Content-Length: ***replaced***
Connection: close
Last-Modified: ***replaced***
Expires: ***replaced***
Expires: ***replaced***
Cache-Control: no-cache, no-store
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'none'; object-src 'none'; base-uri 'none';
↪ connect-src 'self'; script-src 'self'; script-src-elem 'self' 'unsafe-inline'
↪;frame-ancestors 'none'; form-action 'self'; style-src-elem 'self' 'unsafe-inl
↪ine'; style-src 'self' 'unsafe-inline'; font-src 'self';img-src 'self' blob:;
Access-Control-Allow-Origin: gsm.gbuser.net
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
```

Solution:
Solution type: Workaround
Enable HPKP or add / configure the required directives correctly following the guides linked in the references.
Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code.
- Apache: Use 'Header always set' instead of 'Header set'.
- nginx: Append the 'always' keyword to each 'add_header' directive.
For different applications or web severs please refer to the related documentation for a similar configuration possibility.

Log Method
Details: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing
OID:1.3.6.1.4.1.25623.1.0.108247
Version used: 2024-02-08T05:05:59Z

... continues on next page ...

... continued from previous page ...

References

```
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-
↪for-http-hpkp
url: https://tools.ietf.org/html/rfc7469
url: https://securityheaders.io/
url: https://httpd.apache.org/docs/current/mod/mod_headers.html#header
url: https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header
```

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing

Summary
The remote web server is not enforcing HTTP Strict Transport Security (HSTS).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote web server is not enforcing HSTS.
HTTP-Banner:
HTTP/1.1 200 OK
Server: nginx
Date: ***replaced***
Content-Type: text/html; charset=utf-8
Content-Length: ***replaced***
Connection: close
Last-Modified: ***replaced***
Expires: ***replaced***
Expires: ***replaced***
Cache-Control: no-cache, no-store
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'none'; object-src 'none'; base-uri 'none';
↪ connect-src 'self'; script-src 'self'; script-src-elem 'self' 'unsafe-inline'
↪;frame-ancestors 'none'; form-action 'self'; style-src-elem 'self' 'unsafe-inl
↪ine'; style-src 'self' 'unsafe-inline'; font-src 'self';img-src 'self' blob:;
Access-Control-Allow-Origin: gsm.gbuser.net
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
```

Solution:
Solution type: Workaround

... continues on next page ...

... continued from previous page ...

Enable HSTS or add / configure the required directives correctly following the guides linked in the references.
Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code.
- Apache: Use 'Header always set' instead of 'Header set'.
- nginx: Append the 'always' keyword to each 'add_header' directive.
For different applications or web severs please refer to the related documentation for a similar configuration possibility.

Log Method
Details: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing
OID:1.3.6.1.4.1.25623.1.0.105879
Version used: 2024-02-08T05:05:59Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
url: https://owasp.org/www-project-secure-headers/#http-strict-transport-security-hsts
url: https://tools.ietf.org/html/rfc6797
url: https://securityheaders.io/
url: https://httpd.apache.org/docs/current/mod/mod_headers.html#header
url: https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

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

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.802067)

Summary
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Quality of Detection (QoD): 98%

Vulnerability Detection Result
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384

... continues on next page ...

... continued from previous page ...

TLS_CHACHA20_POLY1305_SHA256

Solution:

Log Method
Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: 2024-09-30T08:38:05Z

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

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

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

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256

Solution:

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

... continues on next page ...

... continued from previous page ...

Version used: 2024-09-27T05:05:23Z

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

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

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

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
'Non Weak' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

Solution:

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: 2024-09-27T05:05:23Z

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

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

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result
```
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_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_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.
'Strong' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
No 'Weak' cipher suites accepted by this service via the TLSv1.3 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.3 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.3 protocol.
```

Solution:

Vulnerability Insight
Notes:
- As the VT '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 VT instead.
- SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Log Method
Details: `SSL/TLS: Report Supported Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: `2024-09-27T05:05:23Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: Safe/Secure Renegotiation Support Status

Summary
Checks and reports if a remote SSL/TLS service supports safe/secure renegotiation.

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
Protocol Version | Safe/Secure Renegotiation Support Status
-------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪-------------------------------------
SSLv3            | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.0          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.1          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.2          | Enabled, Note: While the remote service announces the support
↪ of safe/secure renegotiation it still might not support / accept renegotiatio
↪n at all.
TLSv1.3          | Disabled (The TLSv1.3 protocol generally doesn't support rene
↪gotiation so this is always reported as 'Disabled')
```

Solution:

Log Method

Details: SSL/TLS: Safe/Secure Renegotiation Support Status
OID:1.3.6.1.4.1.25623.1.0.117757
Version used: 2024-09-27T05:05:23Z

References

url: https://www.gnutls.org/manual/html_node/Safe-renegotiation.html
url: https://wiki.openssl.org/index.php/TLS1.3#Renegotiation
url: https://datatracker.ietf.org/doc/html/rfc5746

Log (CVSS: 0.0)
NVT: SSL/TLS: Untrusted Certificate Detection

Summary

Checks and reports if a remote SSL/TLS service is using a certificate which is untrusted / the verification against the system wide trust store has failed.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

The remote SSL/TLS server is using the following certificate(s) which failed the

... continues on next page ...

... continued from previous page ...

↪ verification against the system wide trust store (serial:issuer):
0CC5B263F56BB28519DD46EB06981D5225624BD1:C=DE,ST=Niedersachsen,L=Osnabrueck,O=Gr
↪eenbone AG Customer,OU=Vulnerability Management Team,CN=gsm.gbuser.net (Server
↪ certificate)

Solution:

Log Method
Details: SSL/TLS: Untrusted Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.117764
Version used: 2024-09-27T05:05:23Z

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: nginx | Invalid HTTP 00.5 GET request (non-existent HTTP version) to '/'

Solution:

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

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Header Name             | Header Value
------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪-----------------------------------------------------------------------------
Content-Security-Policy | default-src 'none'; object-src 'none'; base-uri 'none'
↪; connect-src 'self'; script-src 'self'; script-src-elem 'self' 'unsafe-inline
↪';frame-ancestors 'none'; form-action 'self'; style-src-elem 'self' 'unsafe-in
↪line'; style-src 'self' 'unsafe-inline'; font-src 'self';img-src 'self' blob
X-Content-Type-Options  | nosniff
X-Frame-Options         | SAMEORIGIN<newline>X-Frame-Options
X-XSS-Protection        | 1; mode=block
Missing Headers                   | More Information
------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪----------
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
Expect-CT                         | https://owasp.org/www-project-secure-headers
↪/#expect-ct, Note: This is an upcoming 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
Public-Key-Pins                   | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
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
```

... continues on next page ...

... continued from previous page ...

```
↪/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
Strict-Transport-Security         | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
```

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: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
A TLScustom server answered 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: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

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

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: SSL/TLS: Version Detection

Summary
Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The remote SSL/TLS service supports the following SSL/TLS protocol version(s):
TLSv1.2
TLSv1.3
```

Solution:

Log Method
Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers.
Details: `SSL/TLS: Version Detection`
OID:1.3.6.1.4.1.25623.1.0.105782

. . . continues on next page . . .

... continued from previous page ...

Version used: 2024-09-27T05:05:23Z

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.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)              | D3C255C6D78958DDE7DAD760D290E990E4C02A08
fingerprint (SHA-256)            | 2033B1DCFC10EC3189B15C5E6CE7791BB257D53783A03B
↪55CBD9C612393B4860
issued by                        | C=DE,ST=Niedersachsen,L=Osnabrueck,O=Greenbone
↪ AG Customer,OU=Vulnerability Management Team,CN=gsm.gbuser.net
public key algorithm             | RSA
public key size (bits)           | 3072
serial                           | 0CC5B263F56BB28519DD46EB06981D5225624BD1
signature algorithm              | sha256WithRSAEncryption
subject                          | C=DE,ST=Niedersachsen,L=Osnabrueck,O=Greenbone
↪ AG Customer,OU=Vulnerability Management Team,CN=gsm.gbuser.net
subject alternative names (SAN)  | gsm.gbuser.net
valid from                       | 2025-02-07 07:40:09 UTC
valid until                      | 2027-02-07 07:40:09 UTC
```

Solution:

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

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.

Quality of Detection (QoD): 80%

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
The service is responding with a 200 HTTP status code to non-existent files/urls
↪. The following pattern is used to work around possible false detections:
-----
Greenbone Enterprise Appliance
-----
```

Solution:

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, authentication page or redirect 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: `2023-07-07T05:05:26Z`

Log (CVSS: 0.0)
NVT: Greenbone Security Assistant (GSA) Detection (HTTP)

Summary

HTTP based detection of the Greenbone Security Assistant (GSA).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Detected Greenbone Security Assistant (GSA)
Version:        unknown
Location:       /
CPE:            cpe:/a:greenbone:greenbone_security_assistant
```

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: Greenbone Security Assistant (GSA) Detection (HTTP)
OID:1.3.6.1.4.1.25623.1.0.103841
Version used: 2024-06-12T05:05:44Z

References
url: https://github.com/greenbone/gsa

[return to 192.168.2.106]

2.6.5 Log 80/tcp

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 "192.168.2.106" 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 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.
```

... continues on next page ...

... continued from previous page ...

```
The following directories were used for web application scanning:
http://192.168.2.106/
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
```

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: 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: nginx | Invalid HTTP 00.5 GET request (non-existent HTTP version) to '/'
```

Solution:

Log Method
Details: `HTTP Server Banner Enumeration`
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: `2025-01-31T15:39:24Z`

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

... continues on next page ...

... continued from previous page ...

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: 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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The host returns a 30x (e.g. 301) error code when a non-existent file is request ↪ed. Some HTTP-related checks have been disabled.`

Solution:

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, authentication page or redirect 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.

... continues on next page ...

... continued from previous page ...

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: `2023-07-07T05:05:26Z`

[return to 192.168.2.106]

2.6.6 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
`192.168.2.106|cpe:/a:f5:nginx`
`192.168.2.106|cpe:/a:greenbone:greenbone_security_assistant`
`192.168.2.106|cpe:/a:greenbone:gsm_trial`
`192.168.2.106|cpe:/a:ietf:transport_layer_security:1.2`
`192.168.2.106|cpe:/a:ietf:transport_layer_security:1.3`
`192.168.2.106|cpe:/a:nginx:nginx`
`192.168.2.106|cpe:/o:greenbone:greenbone_os:22.04.27`

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

[return to 192.168.2.106]

2.7 192.168.2.105

Host scan start	Thu Mar 6 04:48:48 2025 UTC
Host scan end	Thu Mar 6 05:58:33 2025 UTC

Service (Port)	Threat Level
general/icmp	Low
general/tcp	Log
general/CPE-T	Log

2.7.1 Low general/icmp

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

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
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

. . . continues on next page . . .

... continued from previous page ...

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 192.168.2.105]

2.7.2 Log general/tcp

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:           Linux Kernel
CPE:          cpe:/o:linux:kernel
Found by VT:  1.3.6.1.4.1.25623.1.0.102002 (Operating System (OS) Detection (ICM
↪P))
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
```

Solution:

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 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 (192.168.2.108) to target (192.168.2.105):
192.168.2.108
192.168.2.105
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`

Log (CVSS: 0.0)
NVT: IP Forwarding Enabled - Active Check

Summary
Checks if the remote host has IP forwarding enabled.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
```
It was possible to route an ICMP packet through the target host and received an
↪answer which means IP forwarding is enabled.
```

Solution:

Log Method
Sends a crafted Local Link Layer (LLL) frame and checks the response.
Details: `IP Forwarding Enabled - Active Check`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.147205
Version used: 2021-12-03T08:27:06Z

References
cve: CVE-1999-0511

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 192.168.2.105:
Hostname|Source
192.168.2.105|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

[return to 192.168.2.105]

2.7.3 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

... continues on next page ...

... continued from previous page ...

192.168.2.105|cpe:/o:linux:kernel

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

[return to 192.168.2.105]

2.8 192.168.2.61

Host scan start Thu Mar 6 05:24:48 2025 UTC
Host scan end Thu Mar 6 06:11:47 2025 UTC

Service (Port)	Threat Level
general/icmp	Low
general/tcp	Log
general/CPE-T	Log

2.8.1 Low general/icmp

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

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0

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

Solution:

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2025-01-21T05:37:33Z`

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

[return to 192.168.2.61]

2.8.2 Log general/tcp

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:`

... continues on next page ...

... continued from previous page ...

```
OS:           Linux Kernel
CPE:          cpe:/o:linux:kernel
Found by VT:  1.3.6.1.4.1.25623.1.0.102002 (Operating System (OS) Detection (ICM
↪P))
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
```

Solution:

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

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

Log (CVSS: 0.0)
NVT: IP Forwarding Enabled - Active Check

Summary
Checks if the remote host has IP forwarding enabled.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
`It was possible to route an ICMP packet through the target host and received an ↪answer which means IP forwarding is enabled.`

Solution:

Log Method
Sends a crafted Local Link Layer (LLL) frame and checks the response.
Details: `IP Forwarding Enabled - Active Check`
OID:1.3.6.1.4.1.25623.1.0.147205
Version used: `2021-12-03T08:27:06Z`

References
`cve: CVE-1999-0511`

Log (CVSS: 0.0)
NVT: Traceroute

... continues on next page ...

... continued from previous page ...

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 (192.168.2.108) to target (192.168.2.61):
192.168.2.108
192.168.2.61
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`

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 192.168.2.61:
Hostname|Source
192.168.2.61|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`

[return to 192.168.2.61]

2.8.3 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 `192.168.2.61|cpe:/o:linux:kernel`
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 `url: https://nvd.nist.gov/products/cpe`

[return to 192.168.2.61]

2.9 192.168.2.88

Host scan start	Thu Mar 6 02:25:27 2025 UTC
Host scan end	Thu Mar 6 03:44:54 2025 UTC

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

2.9.1 Log general/tcp

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 (192.168.2.108) to target (192.168.2.88):
192.168.2.108
?
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`

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 192.168.2.88:
Hostname|Source
192.168.2.88|IP-address
```

Solution:

Log Method
Details: `Hostname Determination Reporting`

. . . continues on next page . . .

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.108449
Version used: 2022-07-27T10:11:28Z

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:           FreeBSD
CPE:          cpe:/o:freebsd:freebsd
Found by VT:  1.3.6.1.4.1.25623.1.0.102002 (Operating System (OS) Detection (ICM
↪P))
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS:           Apple Mac OS X
CPE:          cpe:/o:apple:mac_os_x
Found by VT:  1.3.6.1.4.1.25623.1.0.102002 (Operating System (OS) Detection (ICM
↪P))
Concluded from ICMP based OS fingerprint
```

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

[return to 192.168.2.88]

2.9.2 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
`192.168.2.88|cpe:/o:freebsd:freebsd`

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

[return to 192.168.2.88]

2.10 192.168.2.20

Host scan start Thu Mar 6 05:00:02 2025 UTC
Host scan end Thu Mar 6 06:06:56 2025 UTC

Service (Port)	Threat Level
general/tcp	Log

2.10.1 Log general/tcp

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.

. . . continues on next page . . .

... continued from previous page ...

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

```
No Best matching OS identified. Please see the VT 'Unknown OS and Service Banner
↪ Reporting' (OID: 1.3.6.1.4.1.25623.1.0.108441) for possible ways to identify
↪this OS.
```

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 (192.168.2.108) to target (192.168.2.20):
192.168.2.108
?
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

... continues on next page ...

. . . continued from previous page . . .

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

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 192.168.2.20:
Hostname|Source
192.168.2.20|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

[return to 192.168.2.20]