Scan Report

November 13, 2024

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 "EdgeMan". The scan started at Mon Oct 14 16:12:13 2024 UTC and ended at Mon Oct 14 17:33:17 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.100.156	0	0	0	25	0
Total: 1	0	0	0	25	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.
Only results with a minimum QoD of 70 are shown.

This report contains all 25 results selected by the filtering described above. Before filtering there were 28 results.

2 Results per Host

2.1 192.168.100.156

Host scan start	Mon Oct 14 16:13:30 2024 UTC
Host scan end	Mon Oct 14 17:33:13 2024 UTC

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

2.1.1 Log general/tcp

Log (CVSS: 0.0)
NVT: nginx Detection Consolidation

Summary
Consolidation of nginx detections.

. . . continues on next page . . .

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
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://192.168.100.156/
```

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: 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:           HP JetDirect
CPE:          cpe:/h:hp:jetdirect
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
```

... 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: `2024-08-02T05:05:39Z`

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 (192.168.138.129) to target (192.168.100.156):
192.168.138.129
192.168.100.156
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

... continues on next page ...

... continued from previous page ...

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 192.168.100.156:
Hostname|Source
192.168.100.156|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 192.168.100.156]

2.1.2 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

```
192.168.100.156|cpe:/a:f5:nginx
192.168.100.156|cpe:/a:ietf:transport_layer_security:1.2
192.168.100.156|cpe:/a:ietf:transport_layer_security:1.3
192.168.100.156|cpe:/a:nginx:nginx
192.168.100.156|cpe:/h:hp:jetdirect
```

Solution:

Log Method

Details: `CPE Inventory`

... continues on next page ...

... continued from previous page ...

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 192.168.100.156]

2.1.3 Log 80/tcp

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

... continues on next page ...

... continued from previous page ...

↪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 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: 2022-06-28T10:11:01Z

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 "192.168.100.156" 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 22.04.22)" 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://192.168.100.156/
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: 2024-08-02T05:05:39Z

References

. . . continues on next page . . .

... continued from previous page ...

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

[return to 192.168.100.156]

2.1.4 Log 443/tcp

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:

... 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: 2024-07-24T05:06:37Z

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)             | A1211F50A04C93244031733923B40AA578358F35
fingerprint (SHA-256)           | 33C79B48C0F5AC8C479842265D397C01282370B3C1454D
↪931B050DFE08C78FC6
issued by                       | CN=Industiral Intermediate Certificate,OU=,O=,
↪STREET=,L=,ST=,C=Edge
public key algorithm            | RSA
public key size (bits)          | 4096
serial                          | 00E5C967FD
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=192.168.100.156,OU=,O=,STREET=,L=,ST=,C=Edg
↪e
subject alternative names (SAN) | localhost
valid from                      | 2024-10-03 10:23:13 UTC
valid until                     | 2034-10-03 10:23:13 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: 2024-06-14T05:05:48Z

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`

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: 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
-------------------------------------------------------------------------
Referrer-Policy            | strict-origin
Strict-Transport-Security  | max-age=63072000; includeSubDomains; preload
X-Content-Type-Options     | nosniff
X-XSS-Protection           | 0
x-frame-options            | SAMEORIGIN
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
```

... continues on next page ...

... continued from previous page ...

```
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.
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: SSL/TLS: HTTP Strict Transport Security (HSTS) Detection

Summary
Checks if the remote web server has HTTP Strict Transport Security (HSTS) enabled.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote web server is sending the "HTTP Strict-Transport-Security" header.

... continues on next page ...

... continued from previous page ...

```
HSTS-Header:
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
```

Solution:

Log Method
Details: SSL/TLS: HTTP Strict Transport Security (HSTS) Detection
OID:1.3.6.1.4.1.25623.1.0.105876
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/

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/1.1 302 Moved Temporarily
Date: ***replaced***
Content-Type: text/html
Content-Length: ***replaced***
Connection: close
x-frame-options: SAMEORIGIN
X-XSS-Protection: 0
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Referrer-Policy: strict-origin
Set-Cookie: ***replaced***|1728927365|1Ti9aRNrbd2zMxl1PjPgDeWWpi9Pwq0kbRI0kFRMpo
↪L3UT1zzixPq-MUU3JdpB0GW9skiN94dJ35CxC7NajGHCctEpvtO3ZqxFgwBpLUKrZvFbilfipxYt6S
↪eAjx48qljzATCDqm9IxxavHKzI11ZoXkC0REIWWofDw6_g_wHxPBKk3q0dP-UpVlMhMoZRzK|1TQxv
↪gpOB03899yUQLPhAE1oyhM; Path=/; SameSite=Lax; Secure; HttpOnly
Cache-Control: no-cache, no-store, max-age=0
```

... continues on next page ...

... continued from previous page ...

```
Location: https://192.168.100.156/auth/realms/customer/protocol/openid-connect/a
↪uth?state=f926561c9a2db93348b5e12dae45a9f3&client_id=ie-management&redirect_ur
↪i=https%3A%2F%2F192.168.100.156%2Fcb&nonce=eecc1aa52aa9268f62e67814f2581bf8&re
↪sponse_type=code&scope=openid
```

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 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%

... continues on next page ...

... continued from previous page ...

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_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
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: 2024-06-14T05:05:48Z

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_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

... continues on next page ...

... continued from previous page ...

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

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_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
'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

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: 2024-06-14T05:05:48Z

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
'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_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:

... continues on next page ...

... continued from previous page ...

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

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          | 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: 2024-07-24T05:06:37Z

... continues on next page ...

... continued from previous page ...

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: 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 "192.168.100.156" 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 22.04.22)" 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 files/directories require authentication and are tested (if enable
↪d) by the script "HTTP Brute Force Logins with default Credentials (OID: 1.3.6
↪.1.4.1.25623.1.0.108041)":
https://192.168.100.156/v2
The following directories were used for web application scanning:
https://192.168.100.156/
https://192.168.100.156/auth/realms/customer/protocol/openid-connect
https://192.168.100.156/osbar/iema-os-bar

... continues on next page ...

... continued from previous page ...

```
https://192.168.100.156/webui
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://192.168.100.156/auth/resources/vgiwz/login/custom/css
https://192.168.100.156/auth/resources/vgiwz/login/custom/img
https://192.168.100.156/auth/resources/vgiwz/login/custom/js
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
https://192.168.100.156/auth/realms/customer/protocol/openid-connect/auth (state
↪ [3db2146f32776a887e8a23446e01fa1f] client_id [ie-management] redirect_uri [ht
↪tps%3A%2F%2F192.168.100.156%2Fcb] nonce [81dfcf55481a6718e576a39c2c3bfa5a] res
↪ponse_type [code] scope [openid] )
```

Solution:

Log Method
Details: Web Application Scanning Consolidation / Info Reporting
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2024-08-02T05:05:39Z

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

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):
00E5C967FD:CN=Industiral Intermediate Certificate,OU=,O=,STREET=,L=,ST=,C=Edge (
↪Server certificate)
00CFAA841A:CN=Industiral,OU=,O=,STREET=,L=,ST=,C=Edge (Certificate in chain)
009A246159:CN=Industiral,OU=,O=,STREET=,L=,ST=,C=Edge (Certificate in chain)
```

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: SSL/TLS: Untrusted Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.117764
Version used: 2024-07-24T05:06:37Z

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 ALPN extension:
SSL/TLS Protocol:Network Protocol
TLSv1.2:HTTP/1.1

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: 2023-04-18T10:19:20Z

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

[return to 192.168.100.156]