

Scan Report

January 22, 2020

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “yo1579635960task”.Thescanstartedatanden01 : 352020UTC.Thereportfirstsummarisestheresultsfound.Then, foreachhost, thereportdescribeseveryissuefound.Please

Contents

1	Result Overview	2
2	Results per Host	2
2.1	127.0.0.1	2
2.1.1	High 9390/tcp	2
2.1.2	Log general/CPE-T	3
2.1.3	Log general/tcp	4
2.1.4	Log 7070/tcp	6
2.1.5	Log 9390/tcp	8
2.1.6	Log 12345/tcp	13
2.1.7	Log 80/tcp	14
2.1.8	Log 631/tcp	16
2.1.9	Log 12346/tcp	29

1 Result Overview

Host	High	Medium	Low	Log	False Positive
127.0.0.1 localhost	1	0	0	39	0
Total: 1	1	0	0	39	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 40 results selected by the filtering described above. Before filtering there were 40 results.

2 Results per Host

2.1 127.0.0.1

Host scan start Tue Jan 21 22:44:18 2020 UTC
Host scan end Tue Jan 21 23:01:35 2020 UTC

Service (Port)	Threat Level
9390/tcp	High
general/CPE-T	Log
general/tcp	Log
7070/tcp	Log
9390/tcp	Log
12345/tcp	Log
80/tcp	Log
631/tcp	Log
12346/tcp	Log

2.1.1 High 9390/tcp

<p>High (CVSS: 10.0) NVT: OpenVAS / Greenbone Vulnerability Manager Default Credentials</p>
<p>Product detection result cpe:/a:openvas:openvas_manager:7.0 Detected by OpenVAS / Greenbone Vulnerability Manager Detection (OID: 1.3.6.1.4.1.25623.1.0.103825)</p>
<p>Summary The remote OpenVAS / Greenbone Vulnerability Manager is installed/configured in a way that it has account(s) with default passwords enabled.</p>
<p>Vulnerability Detection Result It was possible to login using the following credentials (username:password:role ↪): admin:admin:Admin</p>
<p>Impact This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.</p>
<p>Solution Solution type: Workaround Change the password of the mentioned account(s).</p>
<p>Vulnerability Insight It was possible to login with default credentials: admin/admin, sadmin/changeme, observer/observer or admin/openvas.</p>
<p>Vulnerability Detection Method Try to login with default credentials via the OMP/GMP protocol. Details: OpenVAS / Greenbone Vulnerability Manager Default Credentials OID:1.3.6.1.4.1.25623.1.0.108554 Version used: 2019-09-06T14:17:49+0000</p>
<p>Product Detection Result Product: cpe:/a:openvas:openvas_manager:7.0 Method: OpenVAS / Greenbone Vulnerability Manager Detection OID: 1.3.6.1.4.1.25623.1.0.103825)</p>

[\[return to 127.0.0.1 \]](#)

2.1.2 Log general/CPE-T

Log (CVSS: 0.0) NVT: CPE Inventory
<p>Summary</p> <p>This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.</p> <p>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.</p>
<p>Vulnerability Detection Result</p> <p>127.0.0.1 cpe:/a:apple:cups:2.2.10 127.0.0.1 cpe:/a:openvas:openvas_manager:7.0 127.0.0.1 cpe:/o:linux:kernel</p>
<p>Log Method</p> <p>Details: CPE Inventory OID:1.3.6.1.4.1.25623.1.0.810002 Version used: 2019-10-24T11:29:24+0000</p>
<p>References</p> <p>Other: URL:https://nvd.nist.gov/products/cpe</p>

[\[return to 127.0.0.1 \]](#)

2.1.3 Log general/tcp

Log (CVSS: 0.0) NVT: OS Detection Consolidation and Reporting
<p>Summary</p> <p>This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.</p> <p>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.</p> <p>If any of this information is wrong or could be improved please consider to report these to the referenced community portal.</p>
<p>Vulnerability Detection Result</p> <p>Best matching OS: OS: Linux/Unix CPE: cpe:/o:linux:kernel Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification) Concluded from HTTP Server default page on port 631/tcp: <title>Home - CUPS 2.2.↵10</title></p>
<p>... continues on next page ...</p>

...continued from previous page ...
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 NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification) Concluded from HTTP Server banner on port 631/tcp: Server: CUPS/2.2 IPP/2.1
Log Method Details: OS Detection Consolidation and Reporting OID:1.3.6.1.4.1.25623.1.0.105937 Version used: 2019-12-17T06:24:59+0000
References Other: URL: https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0) NVT: SSL/TLS: Hostname discovery from server certificate
Summary It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.
Vulnerability Detection Result The following additional and resolvable hostnames pointing to a different host i ↪p were detected: csirtadmin-VirtualBox csirtadmin-virtualbox
Log Method Details: SSL/TLS: Hostname discovery from server certificate OID:1.3.6.1.4.1.25623.1.0.111010 Version used: \$Revision: 13774 \$

Log (CVSS: 0.0) NVT: Traceroute
Summary A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.
Vulnerability Detection Result Here is the route from 127.0.0.1 to 127.0.0.1: ... continues on next page ...

...continued from previous page ...
127.0.0.1
Solution Block unwanted packets from escaping your network.
Log Method Details: Traceroute OID:1.3.6.1.4.1.25623.1.0.51662 Version used: 2019-09-09T06:03:58+0000

[\[return to 127.0.0.1 \]](#)

2.1.4 Log 7070/tcp

Log (CVSS: 0.0) NVT: SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing
Summary The remote service is missing support for SSL/TLS cipher suites supporting Perfect Forward Secrecy.
Vulnerability Detection Result The remote service does not support perfect forward secrecy cipher suites.
Log Method Details: SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing OID:1.3.6.1.4.1.25623.1.0.105092 Version used: \$Revision: 4736 \$

Log (CVSS: 0.0) NVT: SSL/TLS: Report Medium Cipher Suites
Summary This routine reports all Medium SSL/TLS cipher suites accepted by a service.
Vulnerability Detection Result 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384
... 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: \$Revision: 4743 \$

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Non Weak Cipher Suites

Summary

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

Vulnerability Detection Result

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

TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA256

TLS_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA256

TLS_RSA_WITH_AES_256_GCM_SHA384

Log Method

Details: SSL/TLS: Report Non Weak Cipher Suites

OID:1.3.6.1.4.1.25623.1.0.103441

Version used: \$Revision: 4736 \$

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Supported Cipher Suites

Summary

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

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

Vulnerability Detection Result

No 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol.

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA256

... continues on next page ...

<p>...continued from previous page ...</p> <p>TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA 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.</p>
<p>Log Method Details: SSL/TLS: Report Supported Cipher Suites OID:1.3.6.1.4.1.25623.1.0.802067 Version used: \$Revision: 11108 \$</p>

<p>Log (CVSS: 0.0) NVT: Unknown OS and Service Banner Reporting</p>
<p>Summary This NVT consolidates and reports the information collected by the following NVTs: - 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 portal.</p>
<p>Vulnerability Detection Result Nmap service detection (unknown) result for this port: ssl realserver 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 7070 127.0.0.1' and submit a possible collected fin ↪ gerprint to the nmap database.</p>
<p>Log Method Details: Unknown OS and Service Banner Reporting OID:1.3.6.1.4.1.25623.1.0.108441 Version used: \$Revision: 12934 \$</p>
<p>References Other: URL:https://community.greenbone.net/c/vulnerability-tests</p>

[\[return to 127.0.0.1 \]](#)

2.1.5 Log 9390/tcp

Log (CVSS: 0.0) NVT: OpenVAS / Greenbone Vulnerability Manager Detection
Summary The script sends a connection request to the server and attempts to determine if it is a OpenVAS Manager (openvasmd) or Greebone Vulnerability Manager (gmvd).
Vulnerability Detection Result Detected OpenVAS Manager Version: 7.0 Location: 9390/tcp CPE: cpe:/a:openvas:openvas_manager:7.0 Concluded from version/product identification result: OMP protocol version request '<GET_VERSION/>', response: <version>7.0</version>
Log Method Details: OpenVAS / Greenbone Vulnerability Manager Detection OID:1.3.6.1.4.1.25623.1.0.103825 Version used: 2019-08-05T07:09:20+0000

Log (CVSS: 0.0) NVT: Service Detection with '<xml/>' Request
Summary This plugin performs service detection. This plugin is a complement of find_service.nasl. It sends a '<xml/>' request to the remaining unknown services and tries to identify them.
Vulnerability Detection Result A OpenVAS / Greenbone Vulnerability Manager supporting the OMP/GMP protocol seem ↵s to be running on this port.
Log Method Details: Service Detection with '<xml/>' Request OID:1.3.6.1.4.1.25623.1.0.108198 Version used: 2019-08-05T07:09:20+0000

Log (CVSS: 0.0) NVT: Services
Summary This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.
Vulnerability Detection Result ... continues on next page ...

...continued from previous page ...

A TLScustom server answered on this port

Log Method

Details: Services

OID:1.3.6.1.4.1.25623.1.0.10330

Version used: 2019-07-08T14:12:44+0000

Log (CVSS: 0.0)

NVT: 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.

Vulnerability Detection Result

The following certificate details of the remote service were collected.

Certificate details:

subject ...: C=DE,L=Osnabrueck,O=OpenVAS Users,CN=csirtadmin-VirtualBox

subject alternative names (SAN):

None

issued by .: C=DE,L=Osnabrueck,O=OpenVAS Users,OU=Certificate Authority for csirtadmin-VirtualBox

serial: 1C09DF55B688961C9CEF2F7E9B17F8A87778BE4F

valid from : 2019-12-22 22:03:10 UTC

valid until: 2021-12-21 22:03:10 UTC

fingerprint (SHA-1): 0442451D30AFC7366F7CBF84C4BB86A08966E70B

fingerprint (SHA-256): 3189884906E05F7861BEF2EBCBA19F362666CEBB22427C53C86305B85
↪1265AE2**Log Method**

Details: SSL/TLS: Collect and Report Certificate Details

OID:1.3.6.1.4.1.25623.1.0.103692

Version used: 2019-04-04T13:38:03+0000

Log (CVSS: 0.0)

NVT: SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing

Summary

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

Vulnerability Detection Result

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

Log Method

... continues on next page ...

...continued from previous page ...

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

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Medium Cipher Suites

Summary

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

Vulnerability Detection Result

'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_128_CCM

TLS_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_AES_256_CCM

TLS_RSA_WITH_AES_256_GCM_SHA384

Vulnerability Insight

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

Log Method

Details: SSL/TLS: Report Medium Cipher Suites

OID:1.3.6.1.4.1.25623.1.0.902816

Version used: \$Revision: 4743 \$

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Non Weak Cipher Suites

Summary

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

Vulnerability Detection Result

'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_RSA_WITH_AES_128_CBC_SHA

... continues on next page ...

...continued from previous page...

```

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

```

Log Method

```

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

```

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Supported Cipher Suites

Summary

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

Vulnerability Detection Result

```

No 'Strong' cipher suites accepted by this service via the TLSv1.0 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
No 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Strong' cipher suites accepted by this service via the TLSv1.1 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
No 'Weak' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384

```

...continues on next page...

...continued from previous page ...
No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.
Log Method Details: SSL/TLS: Report Supported Cipher Suites OID:1.3.6.1.4.1.25623.1.0.802067 Version used: \$Revision: 11108 \$

[\[return to 127.0.0.1 \]](#)

2.1.6 Log 12345/tcp

Log (CVSS: 0.0) NVT: Services
Summary This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.
Vulnerability Detection Result The service closed the connection after 0 seconds without sending any data It might be protected by some TCP wrapper
Log Method Details: Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: 2019-07-08T14:12:44+0000

Log (CVSS: 0.0) NVT: Unknown OS and Service Banner Reporting
Summary This NVT consolidates and reports the information collected by the following NVTs: - 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 portal.
Vulnerability Detection Result Nmap service detection (wrapped) result for this port: tcpwrapped
... continues on next page ...

...continued from previous page ...

Log Method

Details: Unknown OS and Service Banner Reporting

OID:1.3.6.1.4.1.25623.1.0.108441

Version used: \$Revision: 12934 \$

References

Other:

URL:<https://community.greenbone.net/c/vulnerability-tests>[\[return to 127.0.0.1 \]](#)**2.1.7 Log 80/tcp**

Log (CVSS: 0.0)

NVT: CGI Scanning Consolidation

Summary

The script consolidates various information for CGI scanning.

This information is based on the following scripts / settings:

- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use

If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result

The Hostname/IP "localhost" was used to access the remote host.

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the 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; OpenVAS-VT 9.0.3)" was used to access the remote host.

Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.

The following directories were used for CGI scanning:

<http://localhost/>

While this is not, in and of itself, a bug, you should manually inspect these di

... continues on next page ...

...continued from previous page ...
↪rectories to ensure that they are in compliance with company security standard ↪s
Log Method Details: CGI Scanning Consolidation OID:1.3.6.1.4.1.25623.1.0.111038 Version used: 2019-09-23T09:25:24+0000
References Other: URL: https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)																					
NVT: HTTP Security Headers Detection																					
Summary All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.																					
Vulnerability Detection Result <table><tr><td>Header Name</td><td>Header Value</td></tr><tr><td>-----</td><td>-----</td></tr><tr><td>Content-Security-Policy</td><td>: default-src 'self' 'unsafe-inline'; img-src 'self' bl↵ob;; frame-ancestors 'self'</td></tr><tr><td>X-Frame-Options</td><td>: SAMEORIGIN</td></tr><tr><td>Missing Headers</td><td></td></tr><tr><td>-----</td><td></td></tr><tr><td>Referrer-Policy</td><td></td></tr><tr><td>X-Content-Type-Options</td><td></td></tr><tr><td>X-Permitted-Cross-Domain-Policies</td><td></td></tr><tr><td>X-XSS-Protection</td><td></td></tr></table>		Header Name	Header Value	-----	-----	Content-Security-Policy	: default-src 'self' 'unsafe-inline'; img-src 'self' bl↵ob;; frame-ancestors 'self'	X-Frame-Options	: SAMEORIGIN	Missing Headers		-----		Referrer-Policy		X-Content-Type-Options		X-Permitted-Cross-Domain-Policies		X-XSS-Protection	
Header Name	Header Value																				
-----	-----																				
Content-Security-Policy	: default-src 'self' 'unsafe-inline'; img-src 'self' bl↵ob;; frame-ancestors 'self'																				
X-Frame-Options	: SAMEORIGIN																				
Missing Headers																					

Referrer-Policy																					
X-Content-Type-Options																					
X-Permitted-Cross-Domain-Policies																					
X-XSS-Protection																					
Log Method Details: HTTP Security Headers Detection OID:1.3.6.1.4.1.25623.1.0.112081 Version used: 2019-11-08T10:10:55+0000																					
References Other: URL:https://www.owasp.org/index.php/OWASP_Secure-Headers_Project URL:https://www.owasp.org/index.php/OWASP_Secure-Headers_Project#tab=Headers URL:https://securityheaders.io/																					

Log (CVSS: 0.0) NVT: Services
Summary This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.
Vulnerability Detection Result A web server is running on this port
Log Method Details: Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: 2019-07-08T14:12:44+0000

[\[return to 127.0.0.1 \]](#)

2.1.8 Log 631/tcp

Log (CVSS: 0.0) NVT: CGI Scanning Consolidation
Summary The script consolidates various information for CGI scanning. This information is based on the following scripts / settings: - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use If you think any of this information is wrong please report it to the referenced community portal.
Vulnerability Detection Result The Hostname/IP "localhost" was used to access the remote host. Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use. Requests to this service are done via HTTP/1.1. This service seems to be NOT able to host PHP scripts. This service seems to be NOT able to host ASP scripts. The User-Agent "Mozilla/5.0 [en] (X11; U; OpenVAS-VT 9.0.3)" was used to access the remote host. Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning ... continues on next page ...

...continued from previous page...

↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.

The following directories were used for CGI scanning:

```
https://localhost:631/
https://localhost:631/admin
https://localhost:631/admin-bak
https://localhost:631/admin-console
https://localhost:631/admin-old
https://localhost:631/admin.back
https://localhost:631/admin_
https://localhost:631/adminer
https://localhost:631/administration
https://localhost:631/administrator
https://localhost:631/adminuser
https://localhost:631/adminweb
https://localhost:631/classes
https://localhost:631/es
https://localhost:631/help
https://localhost:631/helpdesk
https://localhost:631/printers
```

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 CGIs were discovered:

```
Syntax : cginame (arguments [default value])
https://localhost:631/admin (USER_CANCEL_ANY [] DEBUG_LOGGING [] SHARE_PRINTERS
↪[] REMOTE_ANY [] org.cups.sid [fa292e323ea3cc291684def043154ca0] CHANGESSETTING
↪S [Change Settings] KERBEROS [] OP [config-server] REMOTE_ADMIN [] )
https://localhost:631/admin/ (org.cups.sid [fa292e323ea3cc291684def043154ca0] AD
↪VANCEDSETTINGS [YES] OP [add-printer] )
https://localhost:631/admin/log/access_log ()
https://localhost:631/admin/log/error_log ()
https://localhost:631/admin/log/page_log ()
https://localhost:631/classes/ (CLEAR [Clear] QUERY [] )
https://localhost:631/help/ (SEARCH [Search] CLEAR [Clear] TOPIC [Getting+Starte
↪d] QUERY [] )
https://localhost:631/help/accounting.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] TOPIC [Getting+Started] QUERY [] )
https://localhost:631/help/api-admin.html (SEARCH [Search] CLEAR [Clear] PRINTAB
↪LE [YES] QUERY [] TOPIC [Programming] )
https://localhost:631/help/api-filter.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] QUERY [] TOPIC [Programming] )
https://localhost:631/help/api-ppd.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪ [YES] QUERY [] TOPIC [Programming] )
https://localhost:631/help/api-raster.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] QUERY [] TOPIC [Programming] )
```

...continues on next page...

...continued from previous page...

```

https://localhost:631/help/cgi.html (SEARCH [Search] CLEAR [Clear] PRINTABLE [YE
↪S] TOPIC [Getting+Started] QUERY [] )
https://localhost:631/help/cupspm.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪[YES] QUERY [] TOPIC [Programming] )
https://localhost:631/help/encryption.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] TOPIC [Getting+Started] QUERY [] )
https://localhost:631/help/glossary.html (SEARCH [Search] CLEAR [Clear] PRINTABL
↪E [YES] TOPIC [Getting+Started] QUERY [] )
https://localhost:631/help/kerberos.html (SEARCH [Search] CLEAR [Clear] PRINTABL
↪E [YES] TOPIC [Getting+Started] QUERY [] )
https://localhost:631/help/license.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪ [YES] TOPIC [Getting+Started] QUERY [] )
https://localhost:631/help/man-backend.html (SEARCH [Search] CLEAR [Clear] PRINT
↪ABLE [YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-cancel.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-classes.conf.html (SEARCH [Search] CLEAR [Clear]
↪PRINTABLE [YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-client.conf.html (SEARCH [Search] CLEAR [Clear] P
↪RINTABLE [YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-cups-config.html (SEARCH [Search] CLEAR [Clear] P
↪RINTABLE [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-cups-files.conf.html (SEARCH [Search] CLEAR [Clea
↪r] PRINTABLE [YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-cups-lpd.html (SEARCH [Search] CLEAR [Clear] PRIN
↪TABLE [YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-cups-snmpp.conf.html (TOPIC [Man+Pages] )
https://localhost:631/help/man-cups-snmpp.html (SEARCH [Search] CLEAR [Clear] PRI
↪NTABLE [YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-cups.html (SEARCH [Search] CLEAR [Clear] PRINTABL
↪E [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-cupsaccept.html (SEARCH [Search] CLEAR [Clear] PR
↪INTABLE [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-cupsaddsmb.html (SEARCH [Search] CLEAR [Clear] PR
↪INTABLE [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-cupsctl.html (TOPIC [Man+Pages] )
https://localhost:631/help/man-cupsd-helper.html (SEARCH [Search] CLEAR [Clear]
↪PRINTABLE [YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-cupsd-logs.html (SEARCH [Search] CLEAR [Clear] PR
↪INTABLE [YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-cupsd.conf.html (SEARCH [Search] CLEAR [Clear] PR
↪INTABLE [YES] TOPIC [Man Pages] QUERY [] )
https://localhost:631/help/man-cupsd.html (SEARCH [Search] CLEAR [Clear] PRINTAB
↪LE [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-cupsenable.html (SEARCH [Search] CLEAR [Clear] PR
↪INTABLE [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-cupsfilter.html (TOPIC [Man+Pages] )

```

...continues on next page...

...continued from previous page...

```

https://localhost:631/help/man-cupstestdsc.html (SEARCH [Search] CLEAR [Clear] P
↪RINTABLE [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-cupstestppd.html (SEARCH [Search] CLEAR [Clear] P
↪RINTABLE [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-filter.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-ipptool.html (SEARCH [Search] CLEAR [Clear] PRINT
↪ABLE [YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-ipptoolfile.html (SEARCH [Search] CLEAR [Clear] P
↪RINTABLE [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-lp.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪[YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-lpadmin.html (SEARCH [Search] CLEAR [Clear] PRINT
↪ABLE [YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-lpc.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪[YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-lpinfo.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-lpmove.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-lpoptions.html (SEARCH [Search] CLEAR [Clear] PRI
↪NTABLE [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-lpq.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪[YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-lpr.html (SEARCH [Search] CLEAR [Clear] PRINTABLE
↪[YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-lprm.html (SEARCH [Search] CLEAR [Clear] PRINTABL
↪E [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-lpstat.html (SEARCH [Search] CLEAR [Clear] PRINTA
↪BLE [YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-mime.convvs.html (SEARCH [Search] CLEAR [Clear] PR
↪INTABLE [YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-mime.types.html (SEARCH [Search] CLEAR [Clear] PR
↪INTABLE [YES] QUERY [] TOPIC [Man+Pages] )
https://localhost:631/help/man-notifier.html (SEARCH [Search] CLEAR [Clear] PRIN
↪TABLE [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-ppdc.html (SEARCH [Search] CLEAR [Clear] PRINTABL
↪E [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-ppdcfile.html (TOPIC [Man+Pages] )
https://localhost:631/help/man-ppdhtml.html (SEARCH [Search] CLEAR [Clear] PRINT
↪ABLE [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-ppdi.html (SEARCH [Search] CLEAR [Clear] PRINTABL
↪E [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-ppdmerge.html (SEARCH [Search] CLEAR [Clear] PRIN
↪TABLE [YES] TOPIC [Man+Pages] QUERY [] )
https://localhost:631/help/man-ppdpo.html (SEARCH [Search] CLEAR [Clear] PRINTAB
↪LE [YES] TOPIC [Man+Pages] QUERY [] )

```

...continues on next page...

...continued from previous page...
<pre> https://localhost:631/help/man-printers.conf.html (SEARCH [Search] CLEAR [Clear] ↪ PRINTABLE [YES] QUERY [] TOPIC [Man+Pages]) https://localhost:631/help/man-subscriptions.conf.html (SEARCH [Search] CLEAR [C ↪lear] PRINTABLE [YES] TOPIC [Man+Pages] QUERY []) https://localhost:631/help/network.html (SEARCH [Search] CLEAR [Clear] PRINTABLE ↪ [YES] TOPIC [Getting+Started] QUERY []) https://localhost:631/help/options.html (SEARCH [Search] CLEAR [Clear] PRINTABLE ↪ [YES] TOPIC [Getting+Started] QUERY []) https://localhost:631/help/overview.html (SEARCH [Search] CLEAR [Clear] PRINTABL ↪E [YES] TOPIC [Getting Started] QUERY []) https://localhost:631/help/policies.html (SEARCH [Search] CLEAR [Clear] PRINTABL ↪E [YES] TOPIC [Getting+Started] QUERY []) https://localhost:631/help/postscript-driver.html (SEARCH [Search] CLEAR [Clear] ↪ PRINTABLE [YES] QUERY [] TOPIC [Programming]) https://localhost:631/help/ppd-compiler.html (SEARCH [Search] CLEAR [Clear] PRIN ↪TABLE [YES] QUERY [] TOPIC [Programming]) https://localhost:631/help/raster-driver.html (SEARCH [Search] CLEAR [Clear] PRI ↪NTABLE [YES] QUERY [] TOPIC [Programming]) https://localhost:631/help/security.html (SEARCH [Search] CLEAR [Clear] PRINTABL ↪E [YES] TOPIC [Getting+Started] QUERY []) https://localhost:631/help/sharing.html (SEARCH [Search] CLEAR [Clear] PRINTABLE ↪ [YES] TOPIC [Getting+Started] QUERY []) https://localhost:631/help/translation.html (SEARCH [Search] CLEAR [Clear] PRINT ↪ABLE [YES] TOPIC [Getting+Started] QUERY []) https://localhost:631/jobs (which_jobs [completed]) https://localhost:631/jobs/ (CLEAR [Clear] QUERY []) https://localhost:631/printers/ (CLEAR [Clear] QUERY []) </pre>
Log Method Details: CGI Scanning Consolidation OID:1.3.6.1.4.1.25623.1.0.111038 Version used: 2019-09-23T09:25:24+0000
References Other: URL: https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: CUPS Version Detection

Summary

Detects the installed version of Common Unix Printing System (CUPS)
This script sends an HTTP GET request and tries to get the version from the response.

Vulnerability Detection Result

Detected CUPS
Version: 2.2.10

... continues on next page ...

...continued from previous page ...	
Location:	/
CPE:	cpe:/a:apple:cups:2.2.10
Concluded from version/product identification result:	
<title>Home - CUPS 2.2.10</title>	
Log Method	
Details: CUPS Version Detection	
OID:1.3.6.1.4.1.25623.1.0.900348	
Version used: 2019-12-17T11:41:26+0000	

Log (CVSS: 0.0)	
NVT: HTTP Security Headers Detection	
Summary	
All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.	
Vulnerability Detection Result	
Header Name	Header Value
-----	-----
Content-Security-Policy	: frame-ancestors 'none'
X-Frame-Options	: DENY
Missing Headers	

Referrer-Policy	
X-Content-Type-Options	
X-Permitted-Cross-Domain-Policies	
X-XSS-Protection	
Log Method	
Details: HTTP Security Headers Detection	
OID:1.3.6.1.4.1.25623.1.0.112081	
Version used: 2019-11-08T10:10:55+0000	
References	
Other:	
URL:https://www.owasp.org/index.php/OWASP_Secure-Headers_Project	
URL:https://www.owasp.org/index.php/OWASP_Secure-Headers_Project#tab=Headers	
URL:https://securityheaders.io/	

Log (CVSS: 0.0)	
NVT: HTTP Server type and version	
Summary	
... continues on next page ...	

...continued from previous page ...
This detects the HTTP Server's type and version.
Vulnerability Detection Result The remote web server type is : CUPS/2.2 IPP/2.1
Solution - Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display' - Be sure to remove common logos like apache_pb.gif. - With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.
Log Method Details: HTTP Server type and version OID:1.3.6.1.4.1.25623.1.0.10107 Version used: 2019-12-17T11:41:26+0000

Log (CVSS: 0.0) NVT: robot(s).txt exists on the Web Server
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.
Vulnerability Detection Result The file 'robots.txt' contains the following: <pre># # This file tells search engines not to index your CUPS server. # User-agent: * Disallow: /</pre>
Solution Solution type: Mitigation Review the content of the robots 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(s).txt exists on the Web Server OID:1.3.6.1.4.1.25623.1.0.10302 Version used: 2019-11-22T13:51:04+0000

Log (CVSS: 0.0) NVT: Services
Summary This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.
Vulnerability Detection Result A TLScustom server answered on this port
Log Method Details: Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: 2019-07-08T14:12:44+0000

Log (CVSS: 0.0) NVT: Services
Summary This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.
Vulnerability Detection Result A web server is running on this port through SSL
Log Method Details: Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: 2019-07-08T14:12:44+0000

Log (CVSS: 0.0) NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection
Summary The SSL/TLS certificate on this port is self-signed.
Vulnerability Detection Result The certificate of the remote service is self signed. Certificate details: subject ...: L=Unknown,ST=Unknown,OU=Unknown,O=csirtadmin-virtualbox,CN=csirtadm ↪in-virtualbox,C=US subject alternative names (SAN): None issued by ..: L=Unknown,ST=Unknown,OU=Unknown,O=csirtadmin-virtualbox,CN=csirtadm ... continues on next page ...

...continued from previous page...

```

↪in-virtualbox,C=US
serial . . . . : 5E247ECB
valid from : 2020-01-19 16:07:39 UTC
valid until: 2030-01-16 16:07:39 UTC
fingerprint (SHA-1): F02D45182C9DC7CDB3F0DA53C794C090C965B121
fingerprint (SHA-256): 9C1FB73C73BF37FB44C52C3D00A26B9CA3A0FD13991C88E9F79CC74CD
↪DB6C888

```

Log Method

Details: SSL/TLS: Certificate - Self-Signed Certificate Detection
 OID:1.3.6.1.4.1.25623.1.0.103140
 Version used: \$Revision: 8981 \$

References

Other:
 URL:http://en.wikipedia.org/wiki/Self-signed_certificate

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.

Vulnerability Detection Result

The following certificate details of the remote service were collected.
 Certificate details:
 subject . . . : C=DE,L=Osnabrueck,O=OpenVAS Users,CN=csirtadmin-VirtualBox
 subject alternative names (SAN):
 None
 issued by . . : C=DE,L=Osnabrueck,O=OpenVAS Users,OU=Certificate Authority for csir
 ↪tadmin-VirtualBox
 serial : 1C09DF55B688961C9CEF2F7E9B17F8A87778BE4F
 valid from : 2019-12-22 22:03:10 UTC
 valid until: 2021-12-21 22:03:10 UTC
 fingerprint (SHA-1): 0442451D30AFC7366F7CBF84C4BB86A08966E70B
 fingerprint (SHA-256): 3189884906E05F7861BEF2EBCBA19F362666CEBB22427C53C86305B85
 ↪1265AE2

Log Method

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

Log (CVSS: 0.0) NVT: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing
Summary The remote web server is not enforcing HPKP.
Vulnerability Detection Result The remote web server is not enforcing HPKP. HTTP-Banner: HTTP/1.1 200 OK Connection: close Content-Language: en Content-Length: ***replaced*** Content-Type: text/html; charset=utf-8 Date: ***replaced*** Last-Modified: ***replaced*** Accept-Encoding: gzip, deflate, identity Server: CUPS/2.2 IPP/2.1 X-Frame-Options: DENY Content-Security-Policy: frame-ancestors 'none'
Solution Solution type: Workaround Enable HPKP or add / configure the required directives correctly following the guides linked in the references.
Log Method Details: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing OID:1.3.6.1.4.1.25623.1.0.108247 Version used: \$Revision: 7391 \$
References Other: URL: https://www.owasp.org/index.php/OWASP_Secure-Headers_Project URL: https://www.owasp.org/index.php/OWASP_Secure-Headers_Project#hpkp URL: https://tools.ietf.org/html/rfc7469 URL: https://securityheaders.io/

Log (CVSS: 0.0) NVT: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing
Summary The remote web server is not enforcing HSTS.
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 Connection: close Content-Language: en Content-Length: ***replaced*** Content-Type: text/html; charset=utf-8 Date: ***replaced*** Last-Modified: ***replaced*** Accept-Encoding: gzip, deflate, identity Server: CUPS/2.2 IPP/2.1 X-Frame-Options: DENY Content-Security-Policy: frame-ancestors 'none'	
Solution Solution type: Workaround Enable HSTS or add / configure the required directives correctly following the guides linked in the references.	
Log Method Details: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing OID:1.3.6.1.4.1.25623.1.0.105879 Version used: \$Revision: 7391 \$	
References Other: URL: https://www.owasp.org/index.php/OWASP_Secure-Headers_Project URL: https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet ↔ URL: https://www.owasp.org/index.php/OWASP_Secure-Headers_Project#hsts URL: https://tools.ietf.org/html/rfc6797 URL: https://securityheaders.io/	
Log (CVSS: 0.0) NVT: SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing	
Summary The remote service is missing support for SSL/TLS cipher suites supporting Perfect Forward Secrecy.	
Vulnerability Detection Result The remote service does not support perfect forward secrecy cipher suites.	
Log Method Details: SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing OID:1.3.6.1.4.1.25623.1.0.105092 Version used: \$Revision: 4736 \$	

Log (CVSS: 0.0) NVT: SSL/TLS: Report Medium Cipher Suites
Summary This routine reports all Medium SSL/TLS cipher suites accepted by a service.
Vulnerability Detection Result 'Medium' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA 'Medium' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CCM TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CCM TLS_RSA_WITH_AES_256_GCM_SHA384
Vulnerability Insight Any cipher suite considered to be secure for only the next 10 years is considered as medium
Log Method Details: SSL/TLS: Report Medium Cipher Suites OID:1.3.6.1.4.1.25623.1.0.902816 Version used: \$Revision: 4743 \$

Log (CVSS: 0.0) NVT: SSL/TLS: Report Non Weak Cipher Suites
Summary This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.
Vulnerability Detection Result 'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA 'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA 'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CCM TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA ... continues on next page ...

...continued from previous page ...

TLS_RSA_WITH_AES_256_CCM
 TLS_RSA_WITH_AES_256_GCM_SHA384

Log Method

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

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Supported Cipher Suites

Summary

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

Vulnerability Detection Result

No 'Strong' cipher suites accepted by this service via the TLSv1.0 protocol.
 'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
 TLS_RSA_WITH_AES_128_CBC_SHA
 TLS_RSA_WITH_AES_256_CBC_SHA
 No 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol.
 No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
 No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
 No 'Strong' cipher suites accepted by this service via the TLSv1.1 protocol.
 'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
 TLS_RSA_WITH_AES_128_CBC_SHA
 TLS_RSA_WITH_AES_256_CBC_SHA
 No 'Weak' cipher suites accepted by this service via the TLSv1.1 protocol.
 No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol.
 No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol.
 No 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol.
 'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
 TLS_RSA_WITH_AES_128_CBC_SHA
 TLS_RSA_WITH_AES_128_CCM
 TLS_RSA_WITH_AES_128_GCM_SHA256
 TLS_RSA_WITH_AES_256_CBC_SHA
 TLS_RSA_WITH_AES_256_CCM
 TLS_RSA_WITH_AES_256_GCM_SHA384
 No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.
 No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
 No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.

Log Method

Details: SSL/TLS: Report Supported Cipher Suites

... continues on next page ...

...continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.802067
 Version used: \$Revision: 11108 \$

[\[return to 127.0.0.1 \]](#)

2.1.9 Log 12346/tcp

Log (CVSS: 0.0)
 NVT: Services

Summary

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

Vulnerability Detection Result

The service closed the connection after 0 seconds without sending any data
 It might be protected by some TCP wrapper

Log Method

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

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

Summary

This NVT consolidates and reports the information collected by the following NVTs:

- 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 portal.

Vulnerability Detection Result

Nmap service detection (wrapped) result for this port: tcpwrapped

Log Method

Details: Unknown OS and Service Banner Reporting
 OID:1.3.6.1.4.1.25623.1.0.108441
 Version used: \$Revision: 12934 \$

References

... continues on next page ...

...continued from previous page ...

Other:

URL: <https://community.greenbone.net/c/vulnerability-tests>

[\[return to 127.0.0.1 \]](#)

This file was automatically generated.