Scan Report

June 21, 2022

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 “HackTheBox: Secret”. The scan started at Sat Jun 11 20:23:08 2022 UTC and ended at Sat Jun 11 21:26:17 2022 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
10.10.11.120	0	0	1	20	0
Total: 1	0	0	1	20	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 21 results selected by the filtering described above. Before filtering there were 29 results.

2 Results per Host

2.1 10.10.11.120

Host scan start	Sat Jun 11 20:23:41 2022 UTC
Host scan end	Sat Jun 11 21:26:12 2022 UTC

Service (Port)	Threat Level
general/tcp	Low
general/icmp	Log
22/tcp	Log
general/CPE-T	Log
80/tcp	Log
general/tcp	Log
3000/tcp	Log

2.1.1 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

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

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: 3866041860
Packet 2: 3866043030
```

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`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2020-08-24T08:40:10Z`

References

```
url: http://www.ietf.org/rfc/rfc1323.txt
url: http://www.ietf.org/rfc/rfc7323.txt
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
```

[return to 10.10.11.120]

2.1.2 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

Summary
The remote host responded to an ICMP timestamp request. 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. This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Solution:

Log Method
Details: ICMP Timestamp Detection
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: 2021-03-23T06:51:29Z

References
cve: CVE-1999-0524
url: http://www.ietf.org/rfc/rfc0792.txt
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658

[return to 10.10.11.120]

2.1.3 Log 22/tcp

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result
An ssh server is running on this port

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Log Method

Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2021-03-15T10:42:03Z`

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

Summary

This detects the SSH Server's type and version by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Vulnerability Detection Result

```
Remote SSH server banner: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.3
Remote SSH supported authentication: password,publickey
Remote SSH text/login banner: (not available)
This is probably:
- OpenSSH
Concluded from remote connection attempt with credentials:
Login:    OpenVASVT
Password: OpenVASVT
```

Solution:

Log Method

Details: `SSH Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: `2021-09-28T06:32:28Z`

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

Summary

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

Vulnerability Detection Result

```
The following options are supported by the remote ssh service:
kex_algorithms:
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nist
↪p384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-gr
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪oup16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256
server_host_key_algorithms:
rsa-sha2-512,rsa-sha2-256,ssh-rsa,ecdsa-sha2-nistp256,ssh-ed25519
encryption_algorithms_client_to_server:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
encryption_algorithms_server_to_client:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
mac_algorithms_client_to_server:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
mac_algorithms_server_to_client:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
compression_algorithms_client_to_server:
none,zlib@openssh.com
compression_algorithms_server_to_client:
none,zlib@openssh.com
```

Solution:

Log Method

Details: `SSH Protocol Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: `2020-08-24T08:40:10Z`

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

Summary

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

Vulnerability Detection Result

```
The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0
SSHv2 Fingerprint(s):
ecdsa-sha2-nistp256: 95:ed:65:8d:cd:08:2b:55:dd:17:51:31:1e:3e:18:12
ssh-ed25519: 33:7b:c1:71:d3:33:0f:92:4e:83:5a:1f:52:02:93:5e
ssh-rsa: 97:af:61:44:10:89:b9:53:f0:80:3f:d7:19:b1:e2:9c
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:

Log Method
Details: `SSH Protocol Versions Supported`
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: `2020-08-24T08:40:10Z`

[return to 10.10.11.120]

2.1.4 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.

Vulnerability Detection Result
```
10.10.11.120|cpe:/a:f5:nginx:1.18.0
10.10.11.120|cpe:/a:nginx:nginx:1.18.0
10.10.11.120|cpe:/a:openbsd:openssh:8.2p1
10.10.11.120|cpe:/o:canonical:ubuntu_linux:20.04
```

Solution:

Log Method
Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `2021-04-16T10:39:13Z`

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

[return to 10.10.11.120]

2.1.5 Log 80/tcp

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result

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

Solution:

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2021-03-15T10:42:03Z`

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.

Vulnerability Detection Result

```
The remote HTTP Server banner is:
Server: nginx/1.18.0 (Ubuntu)
```

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2020-08-24T15:18:35Z`

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).

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
It was possible to enumerate the following HTTP server banner(s):
Server banner                 | Enumeration technique
-------------------------------------------------------------------------
Server: nginx/1.18.0 (Ubuntu) | Valid HTTP 0.9 GET request to '/index.html'
X-Powered-By: Express         | Valid HTTP 1.0 GET request to '/index.htm'
```

Solution:

Log Method

Details: HTTP Server Banner Enumeration
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: 2021-01-11T11:29:35Z

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.

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪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: 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

. . . 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 portal.

Vulnerability Detection Result

```
The Hostname/IP "10.10.11.120" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 21.4.4)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
A possible recursion was detected during CGI scanning:
The service is using a relative URL in one or more HTML references where e.g. /f
↪ile1.html contains <a href="subdir/file2.html"> and a subsequent request for s
↪ubdir/file2.html is linking to subdir/file2.html. This would resolves to subdi
↪r/subdir/file2.html causing a recursion. To work around this counter-measures
↪have been enabled but the service should be fixed as well to not use such prob
↪lematic links. Below an excerpt of URLs is shown to help identify those issues
↪.
Syntax : URL (HTML link)
http://10.10.11.120/assets/plugins/ (assets/css/theme.css)
http://10.10.11.120/assets/plugins/favicon.ico (assets/css/theme.css)
http://10.10.11.120/assets/plugins/gumshoe/ (assets/css/theme.css)
http://10.10.11.120/assets/plugins/gumshoe/favicon.ico (assets/css/theme.css)
http://10.10.11.120/assets/plugins/simplelightbox/ (assets/css/theme.css)
The following directories were used for CGI scanning:
http://10.10.11.120/
http://10.10.11.120/api
http://10.10.11.120/api/1
http://10.10.11.120/api/2
http://10.10.11.120/api/2.1
http://10.10.11.120/api/2.1/rest
http://10.10.11.120/api/explorer
http://10.10.11.120/api/json
http://10.10.11.120/api/json/nfausers
http://10.10.11.120/api/jsonws
http://10.10.11.120/api/repos
http://10.10.11.120/api/repos/dashboards
http://10.10.11.120/api/system
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
http://10.10.11.120/api/userrolelist
http://10.10.11.120/api/v1
http://10.10.11.120/api/v1.0
http://10.10.11.120/api/v1/status
http://10.10.11.120/api/v2
http://10.10.11.120/api/v2.0
http://10.10.11.120/api/v3
http://10.10.11.120/api/v3.0
http://10.10.11.120/api/v4
http://10.10.11.120/api/v4.0
http://10.10.11.120/api/v5
http://10.10.11.120/api/v5.0
http://10.10.11.120/assets/plugins
http://10.10.11.120/assets/plugins/gumshoe
http://10.10.11.120/assets/plugins/simplelightbox
http://10.10.11.120/docs
http://10.10.11.120/download
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
The following directories were excluded from CGI scanning because the "Regex pat
↪tern to exclude directories from CGI scanning" setting of the NVT "Global vari
↪able settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\
↪.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|p
↪icture|bilder|thumbnail|media/|skins?/)"
http://10.10.11.120/assets/css
http://10.10.11.120/assets/js
http://10.10.11.120/assets/plugins/bootstrap/js
```

Solution:

Log Method

Details: `CGI Scanning Consolidation`

OID:1.3.6.1.4.1.25623.1.0.111038

Version used: `2021-11-30T10:55:08Z`

References

url: `https://community.greenbone.net/c/vulnerability-tests`

[return to 10.10.11.120]

2.1.6 Log general/tcp

Log (CVSS: 0.0)
NVT: OpenSSH Detection Consolidation

Summary
Consolidation of OpenSSH detections.

Vulnerability Detection Result

```
Detected OpenSSH Server
Version:       8.2p1
Location:      22/tcp
CPE:           cpe:/a:openbsd:openssh:8.2p1
Concluded from version/product identification result:
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.3
```

Solution:

Log Method
Details: `OpenSSH Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.108577
Version used: `2019-05-23T06:42:35Z`

References
url: https://www.openssh.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.

Vulnerability Detection Result

```
Network route from scanner (10.10.16.6) to target (10.10.11.120):
10.10.16.6
10.10.11.120
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: `2021-03-12T14:25:59Z`

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 portal.

Vulnerability Detection Result

```
Best matching OS:
OS:           Ubuntu 20.04
Version:      20.04
CPE:          cpe:/o:canonical:ubuntu_linux:20.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (Operating System (OS) Detection (SSH
↪))
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.
↪3
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS:           Ubuntu
CPE:          cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (Operating System (OS) Detection (HTT
↪P))
Concluded from HTTP Server banner on port 80/tcp: Server: nginx/1.18.0 (Ubuntu)
```

Solution:

Log Method

Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `2022-02-24T09:13:28Z`

References

`url: https://community.greenbone.net/c/vulnerability-tests`

Log (CVSS: 0.0)
NVT: nginx Detection Consolidation

Summary
Consolidation of nginx detections.

Vulnerability Detection Result

```
Detected nginx
Version:       1.18.0
Location:      80/tcp
CPE:           cpe:/a:nginx:nginx:1.18.0
Concluded from version/product identification result:
Server: nginx/1.18.0 (Ubuntu)
```

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: Hostname Determination Reporting

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

Vulnerability Detection Result

```
Hostname determination for IP 10.10.11.120:
Hostname|Source
10.10.11.120|IP-address
```

Solution:

Log Method
Details: Hostname Determination Reporting
OID:1.3.6.1.4.1.25623.1.0.108449
Version used: 2018-11-19T11:11:31Z

[return to 10.10.11.120]

2.1.7 Log 3000/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).

Vulnerability Detection Result

```
It was possible to enumerate the following HTTP server banner(s):
Server banner         | Enumeration technique
-------------------------------------------------------------------
X-Powered-By: Express | Valid HTTP 0.9 GET request to '/index.html'
```

Solution:

Log Method
Details: `HTTP Server Banner Enumeration`
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: `2021-01-11T11:29:35Z`

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.

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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

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: 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)

. . . continues on next page . . .

. . . continued from previous page . . .

- 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 "10.10.11.120" 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 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 21.4.4)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
A possible recursion was detected during CGI scanning:
The service is using a relative URL in one or more HTML references where e.g. /f
↪ile1.html contains <a href="subdir/file2.html"> and a subsequent request for s
↪ubdir/file2.html is linking to subdir/file2.html. This would resolves to subdi
↪r/subdir/file2.html causing a recursion. To work around this counter-measures
↪have been enabled but the service should be fixed as well to not use such prob
↪lematic links. Below an excerpt of URLs is shown to help identify those issues
↪.
Syntax : URL (HTML link)
http://10.10.11.120:3000/assets/plugins/ (assets/css/theme.css)
http://10.10.11.120:3000/assets/plugins/favicon.ico (assets/css/theme.css)
http://10.10.11.120:3000/assets/plugins/gumshoe/ (assets/css/theme.css)
http://10.10.11.120:3000/assets/plugins/gumshoe/favicon.ico (assets/css/theme.cs
↪s)
http://10.10.11.120:3000/assets/plugins/simplelightbox/ (assets/css/theme.css)
The following directories were used for CGI scanning:
http://10.10.11.120:3000/
http://10.10.11.120:3000/api
http://10.10.11.120:3000/api/1
http://10.10.11.120:3000/api/2
http://10.10.11.120:3000/api/2.1
http://10.10.11.120:3000/api/2.1/rest
http://10.10.11.120:3000/api/explorer
http://10.10.11.120:3000/api/json
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
http://10.10.11.120:3000/api/json/nfausers
http://10.10.11.120:3000/api/jsonws
http://10.10.11.120:3000/api/repos
http://10.10.11.120:3000/api/repos/dashboards
http://10.10.11.120:3000/api/system
http://10.10.11.120:3000/api/userrolelist
http://10.10.11.120:3000/api/v1
http://10.10.11.120:3000/api/v1.0
http://10.10.11.120:3000/api/v1/status
http://10.10.11.120:3000/api/v2
http://10.10.11.120:3000/api/v2.0
http://10.10.11.120:3000/api/v3
http://10.10.11.120:3000/api/v3.0
http://10.10.11.120:3000/api/v4
http://10.10.11.120:3000/api/v4.0
http://10.10.11.120:3000/api/v5
http://10.10.11.120:3000/api/v5.0
http://10.10.11.120:3000/assets/plugins
http://10.10.11.120:3000/assets/plugins/gumshoe
http://10.10.11.120:3000/assets/plugins/simplelightbox
http://10.10.11.120:3000/docs
http://10.10.11.120:3000/download
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
The following directories were excluded from CGI scanning because the "Regex pat
↪tern to exclude directories from CGI scanning" setting of the NVT "Global vari
↪able settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\
↪.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|p
↪icture|bilder|thumbnail|media/|skins?/)"
http://10.10.11.120:3000/assets/css
http://10.10.11.120:3000/assets/js
http://10.10.11.120:3000/assets/plugins/bootstrap/js
```

Solution:

Log Method

Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2021-11-30T10:55:08Z

References

url: https://community.greenbone.net/c/vulnerability-tests

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
```

Solution:

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2021-03-15T10:42:03Z`

[return to 10.10.11.120]

This file was automatically generated.