Scan Report

June 10, 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 “6666c2d28ed69bdf1709bc9e-6666c2d38ed69bdf1709bccf-9ddae489”. The scan started at Mon Jun 10 09:10:27 2024 UTC and ended at Mon Jun 10 10:28:30 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
3.110.88.164	0	1	2	17	0
Total: 1	0	1	2	17	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.
Only results with a minimum QoD of 70 are shown.

This report contains all 20 results selected by the filtering described above. Before filtering there were 24 results.

2 Results per Host

2.1 3.110.88.164

Host scan start	Mon Jun 10 09:13:45 2024 UTC
Host scan end	

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

2.1.1 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Quality of Detection: 80

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result

```
The following input fields were identified (URL:input name):
http://3.110.88.164/admin/login/:password
http://3.110.88.164/admin/login/?next=/admin/:password
http://3.110.88.164/login/:loginpassword
http://3.110.88.164/login/?next=/administrator/:loginpassword
```

Impact

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:

Solution type: Workaround

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS

Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'

Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

References

```
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html
```

[return to 3.110.88.164]

2.1.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm

Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2023-10-12T05:05:32Z`

References
```
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4
```

[return to 3.110.88.164]

2.1.3 Low general/tcp

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

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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

Quality of Detection: 80

Vulnerability Detection Result

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 625352504
Packet 2: 625353852
```

Impact

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

Solution:

Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

Affected Software/OS

TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: `TCP Timestamps Information Disclosure`

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: `2023-12-15T16:10:08Z`

References

```
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[return to 3.110.88.164]

2.1.4 Log 80/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI (Web application) 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: 80

Vulnerability Detection Result
```
The Hostname/IP "3.110.88.164" 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; OpenVAS-VT 21.4.3)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://3.110.88.164/
http://3.110.88.164/home
http://3.110.88.164/login
http://3.110.88.164/static
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 VT "Global varia
↪ble 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|pi
↪cture|bilder|thumbnail|media/|skins?/)"
http://3.110.88.164/static/admin/css
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
http://3.110.88.164/static/admin/js
http://3.110.88.164/static/images
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://3.110.88.164/admin/login/ (password [] username [] next [/admin/] csrfmid
↪dlewaretoken [***replaced***] )
```

Solution:

Log Method
Details: `CGI Scanning Consolidation`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-02-08T05:05:59Z`

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

Log (CVSS: 0.0)
NVT: Check open ports

Summary
This plugin checks if the port scanners did not kill a service.

Quality of Detection: 80

Vulnerability Detection Result

```
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by a plugin
```

Solution:

Log Method
Details: `Check open ports`
OID:1.3.6.1.4.1.25623.1.0.10919
Version used: `2023-08-03T05:05:16Z`

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.

. . . continues on next page . . .

. . . continued from previous page . . .

Quality of Detection: 80

Vulnerability Detection Result

```
Header Name                 | Header Value
-----------------------------------------
Cross-Origin-Opener-Policy | same-origin
Referrer-Policy            | same-origin
X-Content-Type-Options     | nosniff
X-Frame-Options            | DENY
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-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
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
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:

. . . continues on next page . . .

. . . continued from previous page . . .

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: 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: 80

Vulnerability Detection Result

```
It was possible to enumerate the following HTTP server banner(s):
Server banner                      | Enumeration technique
---------------------------------------------------------------------------
↪------------------------
Server: WSGIServer/0.2 CPython/3.12.3 | Invalid HTTP 00.5 GET request (non-exist
↪ent 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: HTTP Server type and version

Summary

This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
The remote HTTP Server banner is:
Server: WSGIServer/0.2 CPython/3.12.3
```

Solution:

Log Method

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

Log (CVSS: 0.0)
NVT: Services

Summary

This plugin performs service detection.

Quality of Detection: 80

Vulnerability Detection Result

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

Solution:

Vulnerability Insight

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

Log Method

Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

[return to 3.110.88.164]

2.1.5 Log 22/tcp

Log (CVSS: 0.0)
NVT: Services

Summary

This plugin performs service detection.

. . . continues on next page . . .

. . . continued from previous page . . .

Quality of Detection: 80

Vulnerability Detection Result

```
An ssh 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: SSH Protocol Algorithms Supported

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

```
The following options are supported by the remote SSH service:
kex_algorithms:
sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.or
↪g,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-grou
↪p-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,
↪diffie-hellman-group14-sha256,ext-info-s,kex-strict-s-v00@openssh.com
server_host_key_algorithms:
rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519
encryption_algorithms_client_to_server:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
encryption_algorithms_server_to_client:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openss
↪h.com,aes256-gcm@openssh.com
mac_algorithms_client_to_server:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,h
↪mac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,uma
↪c-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
mac_algorithms_server_to_client:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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: 2024-01-09T05:06:46Z

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.

Quality of Detection: 95

Vulnerability Detection Result

```
The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0
SSHv2 Fingerprint(s):
ecdsa-sha2-nistp256: d6:e9:bd:57:89:fa:8f:65:9e:17:ba:b8:2b:9d:62:48
ssh-ed25519: a8:73:0d:22:8a:be:08:df:ca:d8:b6:cc:fb:3f:24:a4
```

Solution:

Log Method

The following versions are tried: 1.33, 1.5, 1.99 and 2.0.
Details: SSH Protocol Versions Supported
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: 2023-09-27T05:05:31Z

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

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

```
Remote SSH server banner: SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13
Remote SSH supported authentication: publickey
Remote SSH text/login banner: (not available)
This is probably:
- OpenSSH
Concluded from remote connection attempt with credentials:
Login:    OpenVASVT
Password: OpenVASVT
```

Solution:

Vulnerability Insight

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

Log Method

Details: `SSH Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: `2024-05-17T15:38:33Z`

[return to 3.110.88.164]

2.1.6 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
3.110.88.164|cpe:/a:openbsd:openssh:9.6p1
3.110.88.164|cpe:/a:python:python:3.12.3
3.110.88.164|cpe:/o:canonical:ubuntu_linux
```

Solution:

Log Method

Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `2022-07-27T10:11:28Z`

References

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

[return to 3.110.88.164]

2.1.7 Log general/tcp

Log (CVSS: 0.0)
NVT: Hostname Determination Reporting

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

```
Hostname determination for IP 3.110.88.164:
Hostname|Source
3.110.88.164|IP-address
```

Solution:

Log Method

Details: `Hostname Determination Reporting`
OID:1.3.6.1.4.1.25623.1.0.108449
Version used: `2022-07-27T10:11:28Z`

Log (CVSS: 0.0)
NVT: OpenSSH Detection Consolidation

Summary

Consolidation of OpenSSH detections.

. . . continues on next page . . .

. . . continued from previous page . . .

Quality of Detection: 80

Vulnerability Detection Result

```
Detected OpenSSH Server
Version:       9.6p1
Location:      22/tcp
CPE:           cpe:/a:openbsd:openssh:9.6p1
Concluded from version/product identification result:
SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13
```

Solution:

Log Method

Details: `OpenSSH Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.108577
Version used: `2022-03-28T10:48:38Z`

References

`url: https://www.openssh.com/`

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

Summary

This script consolidates the OS information detected by several 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: 80

Vulnerability Detection Result

```
Best matching OS:
OS:           Ubuntu
CPE:          cpe:/o:canonical:ubuntu_linux
Found by VT:  1.3.6.1.4.1.25623.1.0.105586 (Operating System (OS) Detection (SSH
↪ Banner))
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13
Setting key "Host/runs_unixoide" based on this information
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Log Method

Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `2024-06-06T05:05:36Z`

References

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

Log (CVSS: 0.0)
NVT: Python Detection Consolidation

Summary

Consolidation of Python detections.

Quality of Detection: 80

Vulnerability Detection Result

```
Detected Python
Version:       3.12.3
Location:      80/tcp
CPE:           cpe:/a:python:python:3.12.3
Concluded from version/product identification result:
Server: WSGIServer/0.2 CPython/3.12.3
```

Solution:

Log Method

Details: `Python Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.112857
Version used: `2021-07-09T08:01:09Z`

References

`url: https://www.python.org/`

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: 80

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Network route from scanner (10.88.0.3) to target (3.110.88.164):
10.88.0.3
10.206.6.95
10.206.35.21
10.206.32.1
173.255.239.101
23.203.156.50
23.203.156.40
23.32.63.253
95.100.192.218
95.100.192.170
23.223.60.35
23.210.54.173
150.222.192.176
150.222.192.177
150.222.192.140
150.222.192.168
52.95.66.80
52.95.64.178
52.95.64.179
52.95.66.87
52.95.67.208
99.83.76.135
99.83.77.26
3.110.88.164
Network distance between scanner and target: 24
```

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: Unknown OS and Service Banner Reporting

Summary

This VT consolidates and reports the information collected by the following VTs:

. . . continues on next page . . .

. . . continued from previous page . . .

- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

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

Quality of Detection: 80

Vulnerability Detection Result

```
Unknown banners have been collected which might help to identify the OS running
↪on this host. If these banners containing information about the host OS please
↪ report the following information to https://forum.greenbone.net/c/vulnerabili
↪ty-tests/7:
Banner: Server: WSGIServer/0.2 CPython/3.12.3
Identified from: HTTP Server banner on port 80/tcp
```

Solution:

Log Method

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

References

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

[return to 3.110.88.164]

This file was automatically generated.