Scan Report

May 9, 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 "myhobbyscan". The scan started at Thu May 9 14:42:26 2024 UTC and ended at Thu May 9 14:55:13 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
172.16.5.4	1	1	3	0	0
Total: 1	1	1	3	0	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 "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 5 results selected by the filtering described above. Before filtering there were 132 results.

2 Results per Host

2.1 172.16.5.4

Host scan start Thu May 9 14:43:20 2024 UTC
Host scan end

Service (Port)	Threat Level
general/tcp	High
22/tcp	Medium
general/icmp	Low
22/tcp	Low
general/tcp	Low

2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: Operating System (OS) End of Life (EOL) Detection

Product detection result
`cpe:/o:debian:debian_linux:8`
`Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0`
`↪.105937)`

. . . continues on next page . . .

... continued from previous page ...

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

Quality of Detection: 80

Vulnerability Detection Result

```
The "Debian GNU/Linux" Operating System on the remote host has reached the end o
↪f life.
CPE:                cpe:/o:debian:debian_linux:8
Installed version,
build or SP:        8
EOL date:           2020-06-30
EOL info:           https://en.wikipedia.org/wiki/List_of_Debian_releases#Release
↪_table
```

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

Solution:
Solution type: Mitigation
Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

Vulnerability Detection Method
Checks if an EOL version of an OS is present on the target host.
Details: `Operating System (OS) End of Life (EOL) Detection`
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: `2024-02-28T14:37:42Z`

Product Detection Result
Product: `cpe:/o:debian:debian_linux:8`
Method: `OS Detection Consolidation and Reporting`
OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 172.16.5.4]

2.1.2 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Host Key Algorithm(s) (SSH)

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

Quality of Detection: 80

Vulnerability Detection Result
```
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
----------------------------------------------------------------------------
↪---------
ssh-dss            | Digital Signature Algorithm (DSA) / Digital Signature Stand
↪ard (DSS)
```

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

Vulnerability Detection Method
Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: `Weak Host Key Algorithm(s) (SSH)`
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: `2023-10-12T05:05:32Z`

References
`url: https://www.rfc-editor.org/rfc/rfc8332`
`url: https://www.rfc-editor.org/rfc/rfc8709`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6`

[return to 172.16.5.4]

2.1.3 Low general/icmp

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

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

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

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

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

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

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References
`cve: CVE-1999-0524`
`url: https://datatracker.ietf.org/doc/html/rfc792`
`url: https://datatracker.ietf.org/doc/html/rfc2780`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 172.16.5.4]

2.1.4 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).

... continues on next page ...

... continued from previous page ...

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 172.16.5.4]

2.1.5 Low general/tcp

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

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

Quality of Detection: 80

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 18189
Packet 2: 18455

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 172.16.5.4]