

Scan Report

June 2, 2023

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 “momentum”. The scan started at Thu Jun 1 15:23:29 2023 UTC and ended at Thu Jun 1 15:38:18 2023 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	2
2	Results per Host	2
2.1	10.0.2.4	2
2.1.1	Low general/icmp	2
2.1.2	Low general/tcp	3

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.0.2.4	0	0	2	0	0
Total: 1	0	0	2	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 2 results selected by the filtering described above. Before filtering there were 51 results.

2 Results per Host

2.1 10.0.2.4

Host scan start Thu Jun 1 15:24:26 2023 UTC

Host scan end Thu Jun 1 15:38:11 2023 UTC

Service (Port)	Threat Level
general/icmp	Low
general/tcp	Low

2.1.1 Low general/icmp

Low (CVSS: 2.1) NVT: ICMP Timestamp Reply Information Disclosure
Summary The remote host responded to an ICMP timestamp request.
Vulnerability Detection Result The following response / ICMP packet has been received: - ICMP Type: 14 - ICMP Code: 0
... continues on next page ...

...continued from previous page ...

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

[\[return to 10.0.2.4 \]](#)

2.1.2 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.

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:

...continues on next page ...

...continued from previous page...	
Packet 1: 2569439785	
Packet 2: 2569440868	
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: 2023-05-11T09:09:33Z	
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/download/details.aspx?id=9152	

[\[return to 10.0.2.4 \]](#)