

# Scan Report

September 25, 2025

## 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 “Scan”. The scan started at Thu Sep 25 15:40:05 2025 UTC and ended at Thu Sep 25 15:56:49 2025 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

<b>1</b>	<b>Result Overview</b>	<b>2</b>
<b>2</b>	<b>Results per Host</b>	<b>2</b>
2.1	192.168.1.6 . . . . .	2
2.1.1	Low general/tcp . . . . .	2

## 1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.1.6	0	0	1	0	0
Total: 1	0	0	1	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 result 1 of the 1 results selected by the filtering above. Before filtering there were 18 results.

## 2 Results per Host

### 2.1 192.168.1.6

Host scan start Thu Sep 25 15:40:44 2025 UTC

Host scan end Thu Sep 25 15:56:45 2025 UTC

Service (Port)	Threat Level
general/tcp	Low

#### 2.1.1 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323/RFC7323. ... continues on next page ...

...continued from previous page...	
The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 1286442377 Packet 2: 212187692	
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.	
<b>Solution:</b> <b>Solution type:</b> 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.	
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.	
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.	
<b>Vulnerability Detection Method</b> 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	
<b>References</b> url: <a href="https://datatracker.ietf.org/doc/html/rfc1323">https://datatracker.ietf.org/doc/html/rfc1323</a> url: <a href="https://datatracker.ietf.org/doc/html/rfc7323">https://datatracker.ietf.org/doc/html/rfc7323</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a> url: <a href="https://www.fortiguard.com/psirt/FG-IR-16-090">https://www.fortiguard.com/psirt/FG-IR-16-090</a>	

[ [return to 192.168.1.6](#) ]