

# Scan Report

September 29, 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 “Immediate scan of IP 192.168.100.202”. The scan started at Sun Sep 29 15:18:27 2024 UTC and ended at Sun Sep 29 15:22:03 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

<b>1</b>	<b>Result Overview</b>	<b>2</b>
<b>2</b>	<b>Results per Host</b>	<b>2</b>
2.1	192.168.100.202 . . . . .	2
2.1.1	Low general/icmp . . . . .	2

## 1 Result Overview

Host	High	Medium	Low	Log	False Positive
<a href="#">192.168.100.202</a>	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 6 results.

## 2 Results per Host

### 2.1 192.168.100.202

Host scan start Sun Sep 29 15:19:15 2024 UTC

Host scan end Sun Sep 29 15:22:01 2024 UTC

Service (Port)	Threat Level
<a href="#">general/icmp</a>	Low

#### 2.1.1 Low [general/icmp](#)

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following response / ICMP packet has been received: ... continues on next page ...

...continued from previous page...	
<ul style="list-style-type: none"><li>- ICMP Type: 14</li><li>- ICMP Code: 0</li></ul>	
<b>Impact</b>	This information could theoretically be used to exploit weak time-based random number generators in other services.
<b>Solution:</b>	
<b>Solution type:</b> Mitigation	
Various mitigations are possible:	
<ul style="list-style-type: none"><li>- Disable the support for ICMP timestamp on the remote host completely</li><li>- 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)</li></ul>	
<b>Vulnerability Insight</b>	
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.	
<b>Vulnerability Detection Method</b>	
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	
<b>References</b>	
cve: CVE-1999-0524	
url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a>	
url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a>	
cert-bund: CB-K15/1514	
cert-bund: CB-K14/0632	
dfn-cert: DFN-CERT-2014-0658	

[\[ return to 192.168.100.202 \]](#)