

# Scan Report

September 20, 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 home network ”. The scan started at Fri Sep 19 20:22:30 2025 UTC and ended at Fri Sep 19 20:38:57 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	192.168.1.1 . . . . .	2
2.1.1	Medium 443/tcp . . . . .	2
2.1.2	Medium 80/tcp . . . . .	3
2.1.3	Low general/icmp . . . . .	5
2.1.4	Low general/tcp . . . . .	6
2.2	192.168.1.240 . . . . .	7
2.2.1	Low general/tcp . . . . .	7
2.3	192.168.1.115 . . . . .	8
2.3.1	Low general/tcp . . . . .	8
2.3.2	Low general/icmp . . . . .	10
2.4	192.168.1.150 . . . . .	11
2.4.1	Low general/icmp . . . . .	11

## 1 Result Overview

Host	High	Medium	Low	Log	False Positive
<a href="#">192.168.1.1</a> <a href="#">saxlv1r.lan</a>	0	2	2	0	0
<a href="#">192.168.1.240</a> <a href="#">mac.lan</a>	0	0	1	0	0
<a href="#">192.168.1.115</a>	0	0	2	0	0
<a href="#">192.168.1.150</a> <a href="#">pavel.lan</a>	0	0	1	0	0
Total: 4	0	2	6	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 8 results selected by the filtering described above. Before filtering there were 109 results.

## 2 Results per Host

### 2.1 192.168.1.1

Host scan start    Fri Sep 19 20:23:09 2025 UTC

Host scan end     Fri Sep 19 20:38:51 2025 UTC

Service (Port)	Threat Level
<a href="#">443/tcp</a>	Medium
<a href="#">80/tcp</a>	Medium
<a href="#">general/icmp</a>	Low
<a href="#">general/tcp</a>	Low

#### 2.1.1 Medium 443/tcp

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits
<b>Summary</b> The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The remote SSL/TLS server is using the following certificate(s) with a RSA key with less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer): 1024:RSA:00FC79B3E38C68CE15:CN=OpenWrt,L=Unknown,ST=Somewhere,C=ZZ (Server certificate)
<b>Impact</b> Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.
<b>Solution:</b> <b>Solution type:</b> Mitigation Replace the certificate with a stronger key and reissue the certificates it signed.
<b>Vulnerability Insight</b> SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.
<b>Vulnerability Detection Method</b> Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit. Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048. ↪.. OID:1.3.6.1.4.1.25623.1.0.150710 Version used: 2021-12-10T12:48:00Z
<b>References</b> url: <a href="https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf">https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf</a>

[\[ return to 192.168.1.1 \]](#)

### 2.1.2 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP
<b>Summary</b> The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> The following URLs requires Basic Authentication (URL:realm name): http://sax1vr.lan/warehouse/control/main:"Please input your authentication info ↵", charset="UTF-8"
<b>Impact</b> 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.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.
<b>Vulnerability Detection Method</b> 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
<b>References</b> url: <a href="https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management">https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management</a> url: <a href="https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure">https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure</a> url: <a href="https://cwe.mitre.org/data/definitions/319.html">https://cwe.mitre.org/data/definitions/319.html</a>

[\[ return to 192.168.1.1 \]](#)

## 2.1.3 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: - ICMP Type: 14 - ICMP Code: 0
<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: - 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)
<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: 2025-01-21T05:37:33Z
<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

[\[ return to 192.168.1.1 \]](#)

#### 2.1.4 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. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 2799460298 Packet 2: 2799461375
<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
... continues on next page ...

...continued from previous page ...
<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>

[\[ return to 192.168.1.1 \]](#)

2.2 192.168.1.240

Host scan start    Fri Sep 19 20:23:09 2025 UTC  
Host scan end     Fri Sep 19 20:30:23 2025 UTC

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

2.2.1 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. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 797725989 Packet 2: 1886384444
<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.
... continues on next page ...

...continued from previous page ...
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>

[\[ return to 192.168.1.240 \]](#)

2.3 192.168.1.115

Host scan start    Fri Sep 19 20:23:09 2025 UTC  
Host scan end     Fri Sep 19 20:33:28 2025 UTC

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

2.3.1 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<b>Summary</b>
... continues on next page ...



...continued from previous page...
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. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 4249952500 Packet 2: 4249953577
<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 192.168.1.115](#) ]

**2.3.2 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: <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: 2025-01-21T05:37:33Z
<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

[\[ return to 192.168.1.115 \]](#)

## 2.4 192.168.1.150

Host scan start Fri Sep 19 20:23:09 2025 UTC

Host scan end Fri Sep 19 20:24:16 2025 UTC

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

### 2.4.1 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: - ICMP Type: 14 - ICMP Code: 0
<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: - 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)
<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> ... continues on next page ...

...continued from previous page ...

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: 2025-01-21T05:37:33Z

#### 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

[\[ return to 192.168.1.150 \]](#)

---

This file was automatically generated.