

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 20:41:12 2025 UTC and ended at Fri Sep 19 21:40:20 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

1	Result Overview	2
2	Results per Host	2
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	192.168.1.236	7
2.2.1	Medium 135/tcp	7
2.2.2	Low general/tcp	9
2.2.3	Low general/icmp	10
2.3	192.168.1.115	11
2.3.1	Low general/tcp	11
2.3.2	Low general/icmp	12
2.4	192.168.1.240	14
2.4.1	Low general/tcp	14
2.5	192.168.1.150	15
2.5.1	Low general/icmp	15

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.1.1 saxlv1r.lan	0	2	2	0	0
192.168.1.236 win10.lan	0	1	2	0	0
192.168.1.115	0	0	2	0	0
192.168.1.240 mac.lan	0	0	1	0	0
192.168.1.150 pavel.lan	0	0	1	0	0
Total: 5	0	3	8	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 11 results selected by the filtering described above. Before filtering there were 121 results.

2 Results per Host

2.1 192.168.1.1

Host scan start Fri Sep 19 20:41:35 2025 UTC

Host scan end Fri Sep 19 20:56:29 2025 UTC

Service (Port)	Threat Level
443/tcp	Medium
80/tcp	Medium
general/icmp	Low
general/tcp	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
Summary 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.
Quality of Detection (QoD): 80%
Vulnerability Detection Result 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)
Impact Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.
Solution: Solution type: Mitigation Replace the certificate with a stronger key and reissue the certificates it signed.
Vulnerability Insight SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.
Vulnerability Detection Method 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
References url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

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

2.1.2 Medium 80/tcp

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

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

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 (QoD): 80%
Vulnerability Detection Result The following response / ICMP packet has been received: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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: 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

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

2.1.4 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 (QoD): 80%
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: 2800536766 Packet 2: 2800537829
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
... continues on next page ...

...continued from previous page ...

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>
url: <https://www.fortiguard.com/psirt/FG-IR-16-090>

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

2.2 192.168.1.236

Host scan start Fri Sep 19 20:41:35 2025 UTC
Host scan end Fri Sep 19 20:50:07 2025 UTC

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

2.2.1 Medium 135/tcp

Medium (CVSS: 5.0)

NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:
Port: 49664/tcp
 UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
 Endpoint: ncacn_ip_tcp:192.168.1.236[49664]
 Named pipe : lsass
 Win32 service or process : lsass.exe
 Description : SAM access
 UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
 Endpoint: ncacn_ip_tcp:192.168.1.236[49664]
 Annotation: Ngc Pop Key Service

... continues on next page ...

...continued from previous page...	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:192.168.1.236[49664] Annotation: Ngc Pop Key Service UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:192.168.1.236[49664] Annotation: KeyIso Port: 49665/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:192.168.1.236[49665] Port: 49666/tcp UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:192.168.1.236[49666] UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:192.168.1.236[49666] Port: 49667/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:192.168.1.236[49667] Annotation: Windows Event Log Port: 49668/tcp UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:192.168.1.236[49668] UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:192.168.1.236[49668] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:192.168.1.236[49668] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:192.168.1.236[49668] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:192.168.1.236[49668] Port: 49669/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:192.168.1.236[49669] Note: DCE/RPC or MSRPC services running on this host locally were identified. Re- porting this list is not enabled by default due to the possible large size of this list. See the script preferences to enable this reporting.	
Impact	An attacker may use this fact to gain more knowledge about the remote host.
Solution:	
Solution type: Mitigation	
Filter incoming traffic to this ports.	
...continues on next page...	

...continued from previous page ...

Vulnerability Detection Method

Details: DCE/RPC and MSRPC Services Enumeration Reporting

OID:1.3.6.1.4.1.25623.1.0.10736

Version used: 2022-06-03T10:17:07Z

[\[return to 192.168.1.236 \]](#)**2.2.2 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.

Quality of Detection (QoD): 80%**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: 7805028

Packet 2: 7806105

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.

... continues on next page ...

...continued from previous page ...
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/download/details.aspx?id=9152 url: https://www.fortiguard.com/psirt/FG-IR-16-090

[\[return to 192.168.1.236 \]](#)

2.2.3 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 (QoD): 80%
Vulnerability Detection Result 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
... continues on next page ...

...continued from previous page ...

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: 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 192.168.1.236](#)]

2.3 192.168.1.115

Host scan start Fri Sep 19 20:41:35 2025 UTC

Host scan end Fri Sep 19 20:52:13 2025 UTC

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

2.3.1 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 (QoD): 80%

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: 4251085735	
Packet 2: 4251086876	
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/download/details.aspx?id=9152 url: https://www.fortiguard.com/psirt/FG-IR-16-090	

[[return to 192.168.1.115](#)]

2.3.2 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 (QoD): 80%
Vulnerability Detection Result 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: 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

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

2.4 192.168.1.240

Host scan start Fri Sep 19 20:41:35 2025 UTC
 Host scan end Fri Sep 19 20:49:36 2025 UTC

Service (Port)	Threat Level
general/tcp	Low

2.4.1 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 (QoD): 80%
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: 2721372266 Packet 2: 2288741039
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.
... continues on next page ...

...continued from previous page...

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/download/details.aspx?id=9152>

url: <https://www.fortiguard.com/psirt/FG-IR-16-090>

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

2.5 192.168.1.150

Host scan start Fri Sep 19 20:41:35 2025 UTC

Host scan end Fri Sep 19 20:42:57 2025 UTC

Service (Port)	Threat Level
general/icmp	Low

2.5.1 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 (QoD): 80%

Vulnerability Detection Result

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.

...continues on next page ...

...continued from previous page ...

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: 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.