

# Scan Report

September 3, 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 “Very fast scan ”. The scan started at Tue Sep 3 10:01:33 2024 UTC and ended at Tue Sep 3 10:52:21 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	192.168.1. [REDACTED]	2
2.1.1	Medium 443/tcp	2
2.1.2	Low general/tcp	7
2.1.3	Low general/icmp	8
2.2	192.168.1. [REDACTED]	9
2.2.1	Low general/tcp	10
2.2.2	Low general/icmp	11
2.3	192.168.1. [REDACTED]	12
2.3.1	Low general/icmp	12
2.3.2	Low general/tcp	13
2.4	192.168.1. [REDACTED]	14
2.4.1	Low general/icmp	14

## 1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.1. [REDACTED] [REDACTED]	0	2	2	0	0
192.168.1. [REDACTED]	0	0	2	0	0
192.168.1. [REDACTED] [REDACTED]	0	0	2	0	0
192.168.1. [REDACTED] [REDACTED]	0	0	1	0	0
Total: 4	0	2	7	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 9 results selected by the filtering described above. Before filtering there were 117 results.

## 2 Results per Host

### 2.1 192.168.1. [REDACTED]

Host scan start Tue Sep 3 10:02:11 2024 UTC

Host scan end Tue Sep 3 10:52:18 2024 UTC

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

#### 2.1.1 Medium 443/tcp

Medium (CVSS: 5.9)

NVT: SSL/TLS: Report Weak Cipher Suites

... continues on next page ...

...continued from previous page ...
<b>Product detection result</b> cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.↪802067)
<b>Summary</b> This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.
<b>Quality of Detection (QoD): 98%</b>
<b>Vulnerability Detection Result</b> 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_RSA_WITH_SEED_CBC_SHA
<b>Solution:</b> <b>Solution type:</b> Mitigation The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.
<b>Vulnerability Insight</b> These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808) - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000) - 1024 bit RSA authentication is considered to be insecure and therefore as weak - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong
<b>Vulnerability Detection Method</b> Details: SSL/TLS: Report Weak Cipher Suites OID:1.3.6.1.4.1.25623.1.0.103440 Version used: 2024-06-14T05:05:48Z
<b>Product Detection Result</b> Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Report Supported Cipher Suites OID: 1.3.6.1.4.1.25623.1.0.802067)
<b>References</b> cve: CVE-2013-2566
... continues on next page ...

...continued from previous page ...

```
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
    ↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
... continues on next page ...
```

...continued from previous page ...

cert-bund: CB-K15/0802  
cert-bund: CB-K15/0764  
cert-bund: CB-K15/0733  
cert-bund: CB-K15/0667  
cert-bund: CB-K14/0935  
cert-bund: CB-K13/0942  
dfn-cert: DFN-CERT-2023-2939  
dfn-cert: DFN-CERT-2021-0775  
dfn-cert: DFN-CERT-2020-1561  
dfn-cert: DFN-CERT-2020-1276  
dfn-cert: DFN-CERT-2017-1821  
dfn-cert: DFN-CERT-2016-1692  
dfn-cert: DFN-CERT-2016-1648  
dfn-cert: DFN-CERT-2016-1168  
dfn-cert: DFN-CERT-2016-0665  
dfn-cert: DFN-CERT-2016-0642  
dfn-cert: DFN-CERT-2016-0184  
dfn-cert: DFN-CERT-2016-0135  
dfn-cert: DFN-CERT-2016-0101  
dfn-cert: DFN-CERT-2016-0035  
dfn-cert: DFN-CERT-2015-1853  
dfn-cert: DFN-CERT-2015-1679  
dfn-cert: DFN-CERT-2015-1632  
dfn-cert: DFN-CERT-2015-1608  
dfn-cert: DFN-CERT-2015-1542  
dfn-cert: DFN-CERT-2015-1518  
dfn-cert: DFN-CERT-2015-1406  
dfn-cert: DFN-CERT-2015-1341  
dfn-cert: DFN-CERT-2015-1194  
dfn-cert: DFN-CERT-2015-1144  
dfn-cert: DFN-CERT-2015-1113  
dfn-cert: DFN-CERT-2015-1078  
dfn-cert: DFN-CERT-2015-1067  
dfn-cert: DFN-CERT-2015-1038  
dfn-cert: DFN-CERT-2015-1016  
dfn-cert: DFN-CERT-2015-1012  
dfn-cert: DFN-CERT-2015-0980  
dfn-cert: DFN-CERT-2015-0977  
dfn-cert: DFN-CERT-2015-0976  
dfn-cert: DFN-CERT-2015-0960  
dfn-cert: DFN-CERT-2015-0956  
dfn-cert: DFN-CERT-2015-0944  
dfn-cert: DFN-CERT-2015-0937  
dfn-cert: DFN-CERT-2015-0925  
dfn-cert: DFN-CERT-2015-0884  
dfn-cert: DFN-CERT-2015-0881  
dfn-cert: DFN-CERT-2015-0879

...continues on next page ...

...continued from previous page ...

dfn-cert: DFN-CERT-2015-0866  
 dfn-cert: DFN-CERT-2015-0844  
 dfn-cert: DFN-CERT-2015-0800  
 dfn-cert: DFN-CERT-2015-0737  
 dfn-cert: DFN-CERT-2015-0696  
 dfn-cert: DFN-CERT-2014-0977

Medium (CVSS: 5.0)

NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

**Summary**

The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**

The following indicates that the remote SSL/TLS service is affected:  
 Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an  
 ↔ existing / already established SSL/TLS connection

-----  
 ↔-----  
 TLSv1.2 | 10

**Impact**

The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

**Solution:**

**Solution type:** VendorFix

Users should contact their vendors for specific patch information.

A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

**Affected Software/OS**

Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

**Vulnerability Insight**

The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.

Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:

> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.

Both CVEs are still kept in this VT as a reference to the origin of this flaw.

... continues on next page ...

...continued from previous page ...
<b>Vulnerability Detection Method</b> Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection. Details: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) OID:1.3.6.1.4.1.25623.1.0.117761 Version used: 2024-07-24T05:06:37Z
<b>References</b> cve: CVE-2011-1473 cve: CVE-2011-5094 url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego-↪tiation-dos/ url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/ url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation url: https://www.openwall.com/lists/oss-security/2011/07/08/2 cert-bund: WID-SEC-2024-1591 cert-bund: WID-SEC-2024-0796 cert-bund: WID-SEC-2023-1435 cert-bund: CB-K17/0980 cert-bund: CB-K17/0979 cert-bund: CB-K14/0772 cert-bund: CB-K13/0915 cert-bund: CB-K13/0462 dfn-cert: DFN-CERT-2017-1013 dfn-cert: DFN-CERT-2017-1012 dfn-cert: DFN-CERT-2014-0809 dfn-cert: DFN-CERT-2013-1928 dfn-cert: DFN-CERT-2012-1112

[\[ return to 192.168.1.100 \]](#)

2.1.2 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: 160486075
... continues on next page ...

...continued from previous page ...
<b>Packet 2:</b> 160486184
<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>

[\[ return to 192.168.1.100 \]](#)

### 2.1.3 Low general/icmp

Low (CVSS: 2.1) NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> ... continues on next page ...



...continued from previous page ...
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: 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

[\[ return to 192.168.1.100 \]](#)

2.2 192.168.1.100

Host scan start    Tue Sep 3 10:02:11 2024 UTC

Host scan end     Tue Sep 3 10:16:21 2024 UTC

Service (Port)	Threat Level
<a href="#">general/tcp</a>	Low
<a href="#">general/icmp</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: 1025287160 Packet 2: 1025288233
<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
... continues on next page ...

...continued from previous page ...
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>

[\[ return to 192.168.1. \]](#)

### 2.2.2 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: - 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.
... continues on next page ...

...continued from previous page ...
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: 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

[\[ return to 192.168.1.100 \]](#)

2.3 192.168.1.100

Host scan start    Tue Sep 3 10:02:11 2024 UTC  
Host scan end     Tue Sep 3 10:44:09 2024 UTC

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

2.3.1 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
... continues on next page ...

...continued from previous page ...
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> <p>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.</p>
<b>Vulnerability Detection Method</b> <p>Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.</p> <p>Details: ICMP Timestamp Reply Information Disclosure</p> <p>OID:1.3.6.1.4.1.25623.1.0.103190</p> <p>Version used: 2023-05-11T09:09:33Z</p>
<b>References</b> <p>cve: CVE-1999-0524</p> <p>url: <a href="https://datatracker.ietf.org/doc/html/rfc792">https://datatracker.ietf.org/doc/html/rfc792</a></p> <p>url: <a href="https://datatracker.ietf.org/doc/html/rfc2780">https://datatracker.ietf.org/doc/html/rfc2780</a></p> <p>cert-bund: CB-K15/1514</p> <p>cert-bund: CB-K14/0632</p> <p>dfn-cert: DFN-CERT-2014-0658</p>

[\[ return to 192.168.1.100 \]](#)

2.3.2 Low general/tcp

Low (CVSS: 2.6) NVT: TCP Timestamps Information Disclosure
<b>Summary</b> <p>The remote host implements TCP timestamps and therefore allows to compute the uptime.</p>
<b>Quality of Detection (QoD):</b> 80%
<b>Vulnerability Detection Result</b> <p>It was detected that the host implements RFC1323/RFC7323.</p> <p>The following timestamps were retrieved with a delay of 1 seconds in-between:</p> <p>Packet 1: 390456854</p> <p>Packet 2: 390457924</p>
<b>Impact</b> <p>... continues on next page ...</p>

...continued from previous page ...
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>

[\[ return to 192.168.1.100 \]](#)

## 2.4 192.168.1.100

Host scan start    Tue Sep 3 10:02:11 2024 UTC

Host scan end     Tue Sep 3 10:10:02 2024 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: <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

[\[ return to 192.168.1.100 \]](#)

This file was automatically generated.