Scan Report

March 9, 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 "Immediate scan of IP 10.0.0.0/24". The scan started at Sat Mar 8 02:09:33 2025 UTC and ended at Sat Mar 8 14:52:55 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

Host	High	Medium	Low	Log	False Positive
10.0.0.1	0	2	2	0	0
10.0.0.205	0	1	0	0	0
10.0.0.16	0	0	2	0	0
10.0.0.168	0	0	1	0	0
10.0.0.34	0	0	2	0	0
10.0.0.212	0	0	1	0	0
10.0.0.12	0	0	2	0	0
10.0.0.29	0	0	1	0	0
Total: 8	0	3	11	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 14 results selected by the filtering described above. Before filtering there were 198 results.

2 Results per Host

2.1 10.0.0.1

Host scan start	Sat Mar 8 02:14:32 2025 UTC
Host scan end	Sat Mar 8 04:25:16 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: 4.0)

NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Server Temporary Key Size: 1024 bits

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution:
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili...
↪..
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: 2024-09-30T08:38:05Z

References
url: https://weakdh.org/
url: https://weakdh.org/sysadmin.html

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 input fields were identified (URL:input name):`
`http://10.0.0.1/:password`

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_Se`
`↪ssion_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 10.0.0.1]

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:
- 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
```

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: 2249627761
Packet 2: 2249628886
```

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 . . .

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/d ↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090

2.2   10.0.0.205

Host scan start	Sat Mar 8 02:14:32 2025 UTC
Host scan end	Sat Mar 8 14:52:47 2025 UTC

Service (Port)	Threat Level
443/tcp	Medium

2.2.1   Medium 443/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Product detection result cpe:/a:ietf:transport_layer_security:1.0 Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection (QoD): 98%
Vulnerability Detection Result In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and ↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c ↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1 ↪.25623.1.0.802067) VT.
Impact An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-09-27T05:05:23Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security:1.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

References
`cve: CVE-2011-3389`
`cve: CVE-2015-0204`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://datatracker.ietf.org/doc/rfc8996/`
`url: https://vnhacker.blogspot.com/2011/09/beast.html`
`url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters`
`↪-report-2014`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`
`cert-bund: CB-K15/1266`
`cert-bund: CB-K15/0850`

```
cert-bund:  CB-K15/0764
cert-bund:  CB-K15/0720
cert-bund:  CB-K15/0548
cert-bund:  CB-K15/0526
cert-bund:  CB-K15/0509
cert-bund:  CB-K15/0493
cert-bund:  CB-K15/0384
cert-bund:  CB-K15/0365
cert-bund:  CB-K15/0364
cert-bund:  CB-K15/0302
cert-bund:  CB-K15/0192
cert-bund:  CB-K15/0079
cert-bund:  CB-K15/0016
cert-bund:  CB-K14/1342
cert-bund:  CB-K14/0231
cert-bund:  CB-K13/0845
cert-bund:  CB-K13/0796
cert-bund:  CB-K13/0790
dfn-cert:  DFN-CERT-2020-0177
dfn-cert:  DFN-CERT-2020-0111
dfn-cert:  DFN-CERT-2019-0068
dfn-cert:  DFN-CERT-2018-1441
dfn-cert:  DFN-CERT-2018-1408
dfn-cert:  DFN-CERT-2016-1372
dfn-cert:  DFN-CERT-2016-1164
dfn-cert:  DFN-CERT-2016-0388
dfn-cert:  DFN-CERT-2015-1853
dfn-cert:  DFN-CERT-2015-1332
dfn-cert:  DFN-CERT-2015-0884
dfn-cert:  DFN-CERT-2015-0800
dfn-cert:  DFN-CERT-2015-0758
dfn-cert:  DFN-CERT-2015-0567
dfn-cert:  DFN-CERT-2015-0544
dfn-cert:  DFN-CERT-2015-0530
dfn-cert:  DFN-CERT-2015-0396
dfn-cert:  DFN-CERT-2015-0375
dfn-cert:  DFN-CERT-2015-0374
dfn-cert:  DFN-CERT-2015-0305
dfn-cert:  DFN-CERT-2015-0199
dfn-cert:  DFN-CERT-2015-0079
dfn-cert:  DFN-CERT-2015-0021
dfn-cert:  DFN-CERT-2014-1414
dfn-cert:  DFN-CERT-2013-1847
dfn-cert:  DFN-CERT-2013-1792
dfn-cert:  DFN-CERT-2012-1979
dfn-cert:  DFN-CERT-2012-1829
dfn-cert:  DFN-CERT-2012-1530
```

```
dfn-cert:  DFN-CERT-2012-1380
dfn-cert:  DFN-CERT-2012-1377
dfn-cert:  DFN-CERT-2012-1292
dfn-cert:  DFN-CERT-2012-1214
dfn-cert:  DFN-CERT-2012-1213
dfn-cert:  DFN-CERT-2012-1180
dfn-cert:  DFN-CERT-2012-1156
dfn-cert:  DFN-CERT-2012-1155
dfn-cert:  DFN-CERT-2012-1039
dfn-cert:  DFN-CERT-2012-0956
dfn-cert:  DFN-CERT-2012-0908
dfn-cert:  DFN-CERT-2012-0868
dfn-cert:  DFN-CERT-2012-0867
dfn-cert:  DFN-CERT-2012-0848
dfn-cert:  DFN-CERT-2012-0838
dfn-cert:  DFN-CERT-2012-0776
dfn-cert:  DFN-CERT-2012-0722
dfn-cert:  DFN-CERT-2012-0638
dfn-cert:  DFN-CERT-2012-0627
dfn-cert:  DFN-CERT-2012-0451
dfn-cert:  DFN-CERT-2012-0418
dfn-cert:  DFN-CERT-2012-0354
dfn-cert:  DFN-CERT-2012-0234
dfn-cert:  DFN-CERT-2012-0221
dfn-cert:  DFN-CERT-2012-0177
dfn-cert:  DFN-CERT-2012-0170
dfn-cert:  DFN-CERT-2012-0146
dfn-cert:  DFN-CERT-2012-0142
dfn-cert:  DFN-CERT-2012-0126
dfn-cert:  DFN-CERT-2012-0123
dfn-cert:  DFN-CERT-2012-0095
dfn-cert:  DFN-CERT-2012-0051
dfn-cert:  DFN-CERT-2012-0047
dfn-cert:  DFN-CERT-2012-0021
dfn-cert:  DFN-CERT-2011-1953
dfn-cert:  DFN-CERT-2011-1946
dfn-cert:  DFN-CERT-2011-1844
dfn-cert:  DFN-CERT-2011-1826
dfn-cert:  DFN-CERT-2011-1774
dfn-cert:  DFN-CERT-2011-1743
dfn-cert:  DFN-CERT-2011-1738
dfn-cert:  DFN-CERT-2011-1706
dfn-cert:  DFN-CERT-2011-1628
dfn-cert:  DFN-CERT-2011-1627
dfn-cert:  DFN-CERT-2011-1619
dfn-cert:  DFN-CERT-2011-1482
```

[return to 10.0.0.205]

2.3   10.0.0.16

Host scan start   Sat Mar 8 02:14:32 2025 UTC
Host scan end   Sat Mar 8 04:40:16 2025 UTC

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

2.3.1   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.

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`

. . . continues on next page . . .

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 10.0.0.16]

2.3.2 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: 26987387
Packet 2: 26987736

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/d`
`↪ownload/details.aspx?id=9152`
`url: https://www.fortiguard.com/psirt/FG-IR-16-090`

2.4   10.0.0.168

Host scan start	Sat Mar 8 02:14:32 2025 UTC
Host scan end	Sat Mar 8 04:01:43 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: 1979727571
Packet 2: 323887625
```

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/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[return to 10.0.0.168]

2.5   10.0.0.34

Host scan start	Sat Mar 8 02:14:32 2025 UTC
Host scan end	Sat Mar 8 04:34:19 2025 UTC

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

2.5.1   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: 557184
Packet 2: 557306
```

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/d`
↪`ownload/details.aspx?id=9152`
url: `https://www.fortiguard.com/psirt/FG-IR-16-090`

[return to 10.0.0.34]

2.5.2   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`

2.6 10.0.0.212

Host scan start	Sat Mar 8 02:14:32 2025 UTC
Host scan end	Sat Mar 8 03:44:43 2025 UTC

Service (Port)	Threat Level
general/tcp	Low

2.6.1 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: 2203883677
Packet 2: 3508518995

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/d`
`↪ownload/details.aspx?id=9152`
`url: https://www.fortiguard.com/psirt/FG-IR-16-090`

2.7   10.0.0.12

Host scan start   Sat Mar 8 02:14:32 2025 UTC
Host scan end   Sat Mar 8 03:57:16 2025 UTC

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

2.7.1   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: 24214589
Packet 2: 24214867
```

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/d
```

```
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

2.7.2 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 10.0.0.12]

2.8   10.0.0.29

Host scan start   Sat Mar 8 02:14:32 2025 UTC
Host scan end   Sat Mar 8 03:04:54 2025 UTC

Service (Port)	Threat Level
general/icmp	Low

2.8.1   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.

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 10.0.0.29]

This file was automatically generated.