

Scan Report

April 20, 2026

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 “New Quick Task”. The scan started at Mon Apr 20 11:25:46 2026 UTC and ended at Mon Apr 20 13:07:25 2026 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	10.0.0.1	2
2.2	20.0.0.1	2
2.3	20.0.0.2	2
2.4	192.168.1.1	3
2.4.1	Critical 445/tcp	3
2.4.2	Critical 9/tcp	4
2.4.3	High 443/tcp	5
2.4.4	Medium 7/tcp	9
2.4.5	Medium 135/tcp	10
2.4.6	Medium 443/tcp	14
2.4.7	Medium 17/tcp	20
2.4.8	Medium 19/tcp	21
2.4.9	Low general/tcp	22
2.4.10	Low general/icmp	23
2.5	192.168.1.10	24
2.5.1	Medium 135/tcp	24
2.5.2	Low general/icmp	27

1 Result Overview

Host	Critical	High	Medium	Low	Log	False P.
10.0.0.1	0	0	0	0	0	0
20.0.0.1	0	0	0	0	0	0
20.0.0.2	0	0	0	0	0	0
192.168.1.1	2	1	6	2	0	0
192.168.1.10	0	0	1	1	0	0
Total: 5	2	1	7	3	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 13 results selected by the filtering described above. Before filtering there were 113 results.

2 Results per Host

2.1 10.0.0.1

Host scan start Mon Apr 20 11:26:09 2026 UTC
Host scan end Mon Apr 20 11:28:09 2026 UTC

Service (Port)	Threat Level
----------------	--------------

2.2 20.0.0.1

Host scan start Mon Apr 20 11:26:09 2026 UTC
Host scan end Mon Apr 20 13:06:39 2026 UTC

Service (Port)	Threat Level
----------------	--------------

2.3 20.0.0.2

Host scan start Mon Apr 20 11:26:09 2026 UTC
Host scan end Mon Apr 20 13:07:17 2026 UTC

Service (Port)	Threat Level
----------------	--------------

2.4 192.168.1.1

Host scan start Mon Apr 20 11:26:09 2026 UTC
Host scan end Mon Apr 20 12:19:29 2026 UTC

Service (Port)	Threat Level
445/tcp	Critical
9/tcp	Critical
443/tcp	High
7/tcp	Medium
135/tcp	Medium
443/tcp	Medium
17/tcp	Medium
19/tcp	Medium
general/tcp	Low
general/icmp	Low

2.4.1 Critical 445/tcp

Critical (CVSS: 10.0)

NVT: SMB Brute Force Logins With Default Credentials

Summary

A number of known default credentials are tried for the login via the SMB protocol.

Quality of Detection (QoD): 99%

Vulnerability Detection Result

It was possible to login with the following credentials via the SMB protocol to ↪the 'IPC\$' share. <User>:<Password>
ftpuser:123456

Solution:

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Tries to login with a number of known default credentials via the SMB protocol.
Details: SMB Brute Force Logins With Default Credentials
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: 2026-03-18T05:59:10Z

... continues on next page ...

...continued from previous page ...

References

cve: CVE-1999-0503
 cve: CVE-1999-0504
 cve: CVE-1999-0505
 cve: CVE-1999-0506
 cve: CVE-1999-0585
 cve: CVE-2000-0222
 cve: CVE-2005-3595

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

2.4.2 Critical 9/tcp

Critical (CVSS: 10.0)

NVT: Check for discard Service (TCP)

Product detection result

cpe:/a:postel:discard

Detected by discard Service Detection (TCP) (OID: 1.3.6.1.4.1.25623.1.0.113757)

Summary

The remote host is running a 'discard' service. This service typically sets up a listening socket and will ignore all the data which it receives.

This service is unused these days, so it is advised that you disable it.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

The discard service was detected on the target host.

Solution:

Solution type: Mitigation

- Under Unix systems, comment out the 'discard' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry key to 0:

HKLM\System\CurrentControlSet\Services\SimpleTCP\Parameters\EnableTcpDiscard

Then launch cmd.exe and type:

net stop simptcp

net start simptcp

To restart the service.

Notes:

... continues on next page ...

...continued from previous page ...
Some firewall devices are known to discard packets on the checked port 9/tcp or mimic such a service via other means. Scanning through a firewall should be generally avoided (Please see references). If the target was scanned through a firewall and it was determined / has been verified that no such service is running on the target please either: - create an override for this result - configure the firewall in a way that port 9/tcp is not reported as being open during the port scanning phase / it is not allowed to open a TCP connection to port 9/tcp on the target
Vulnerability Detection Method Checks whether a discard service is exposed on the target host by evaluating the info from the following service detection: - discard Service Detection (TCP) (OID: 1.3.6.1.4.1.25623.1.0.113757) Details: Check for discard Service (TCP) OID:1.3.6.1.4.1.25623.1.0.11367 Version used: 2025-01-31T15:39:24Z
Product Detection Result Product: cpe:/a:postel:discard Method: discard Service Detection (TCP) OID: 1.3.6.1.4.1.25623.1.0.113757)
References cve: CVE-1999-0636 url: https://datatracker.ietf.org/doc/html/rfc863 url: https://docs.greenbone.net/GSM-Manual/gos-22.04/en/read-before-use.html#scanning-through-network-equipment

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

2.4.3 High 443/tcp

High (CVSS: 7.5) NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
Product detection result 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)
Summary ... continues on next page ...

...continued from previous page ...
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.
Quality of Detection (QoD): 98%
Vulnerability Detection Result 'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32) 'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32) 'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
Impact This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.
Solution: Solution type: Mitigation The configuration of this services should be changed so that it does not accept the listed cipher suites anymore. Please see the references for more resources supporting you with this task.
Affected Software/OS All services accepting vulnerable SSL/TLS cipher suites via HTTPS.
Vulnerability Insight These rules are applied for the evaluation of the vulnerable cipher suites: - 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).
Vulnerability Detection Method Checks previous collected cipher suites. Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS OID:1.3.6.1.4.1.25623.1.0.108031 Version used: 2026-03-13T05:54:58Z
Product Detection Result 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)
References cve: CVE-2016-2183 cve: CVE-2016-6329 cve: CVE-2020-12872
... continues on next page ...

...continued from previous page...

url: <https://ssl-config.mozilla.org>
 url: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html>
 url: https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/0TLS-Protokoll/TLS-Protokoll_node.html
 url: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html>
 url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html
 url: <https://web.archive.org/web/20240113175943/https://www.bettercrypto.org>
 url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters0-report-2014>
 url: <https://sweet32.info>
 cert-bund: WID-SEC-2026-0180
 cert-bund: WID-SEC-2024-1277
 cert-bund: WID-SEC-2024-0209
 cert-bund: WID-SEC-2024-0064
 cert-bund: WID-SEC-2022-2226
 cert-bund: WID-SEC-2022-1955
 cert-bund: CB-K21/1094
 cert-bund: CB-K20/1023
 cert-bund: CB-K20/0321
 cert-bund: CB-K20/0314
 cert-bund: CB-K20/0157
 cert-bund: CB-K19/0618
 cert-bund: CB-K19/0615
 cert-bund: CB-K18/0296
 cert-bund: CB-K17/1980
 cert-bund: CB-K17/1871
 cert-bund: CB-K17/1803
 cert-bund: CB-K17/1753
 cert-bund: CB-K17/1750
 cert-bund: CB-K17/1709
 cert-bund: CB-K17/1558
 cert-bund: CB-K17/1273
 cert-bund: CB-K17/1202
 cert-bund: CB-K17/1196
 cert-bund: CB-K17/1055
 cert-bund: CB-K17/1026
 cert-bund: CB-K17/0939
 cert-bund: CB-K17/0917
 cert-bund: CB-K17/0915
 cert-bund: CB-K17/0877
 cert-bund: CB-K17/0796
 cert-bund: CB-K17/0724
 cert-bund: CB-K17/0661
 cert-bund: CB-K17/0657

...continues on next page...

...continued from previous page ...

cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2025-0041
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904

...continues on next page ...

...continued from previous page ...

```

dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378

```

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

2.4.4 Medium 7/tcp

Medium (CVSS: 5.0)

NVT: echo Service Reporting (TCP + UDP)

Summary

An echo Service is running at this Host via TCP and/or UDP.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution:

Solution type: Mitigation

Disable the echo Service.

... continues on next page ...

...continued from previous page ...
Vulnerability Insight The echo service is an Internet protocol defined in RFC 862. It was originally proposed for testing and measurement of round-trip times in IP networks. While still available on most UNIX-like operating systems, testing and measurement is now performed with the Internet Control Message Protocol (ICMP), using the applications ping and traceroute.
Vulnerability Detection Method Checks whether an echo service is exposed on the target host. Details: echo Service Reporting (TCP + UDP) OID:1.3.6.1.4.1.25623.1.0.100075 Version used: 2023-09-12T05:05:19Z
References cve: CVE-1999-0103 cve: CVE-1999-0635

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

2.4.5 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 based service enumeration reporting.
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: 3388/tcp UUID: 44e265dd-7daf-42cd-8560-3cdb6e7a2729, version 1 Endpoint: ncacn_http:192.168.1.1[3388] Annotation: TsProxy UUID: 958f92d8-da20-467a-bbe3-65e7e9b4edcf, version 1 Endpoint: ncacn_http:192.168.1.1[3388] Annotation: TsProxyMgmt Port: 49573/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:192.168.1.1[49573] Annotation: RemoteAccessCheck
... continues on next page ...

...continued from previous page...	
UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[49573]	
Named pipe : lsass	
Win32 service or process : Netlogon	
Description : Net Logon service	
UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0	
Endpoint: ncacn_ip_tcp:192.168.1.1[49573]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : LSA access	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[49573]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[49573]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.1.1[49573]	
Annotation: KeyIso	
UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4	
Endpoint: ncacn_ip_tcp:192.168.1.1[49573]	
Annotation: MS NT Directory DRS Interface	
Port: 49664/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_ip_tcp:192.168.1.1[49664]	
Annotation: RemoteAccessCheck	
UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[49664]	
Named pipe : lsass	
Win32 service or process : Netlogon	
Description : Net Logon service	
UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0	
Endpoint: ncacn_ip_tcp:192.168.1.1[49664]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : LSA access	
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[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:192.168.1.1[49664]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[49664]	
Annotation: Ngc Pop Key Service	
...continues on next page...	

...continued from previous page...	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.1.1[49664]	
Annotation: KeyIso	
UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[49664]	
Annotation: Impl friendly name	
UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4	
Endpoint: ncacn_ip_tcp:192.168.1.1[49664]	
Annotation: MS NT Directory DRS Interface	
Port: 49665/tcp	
UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[49665]	
Port: 49666/tcp	
UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[49666]	
Annotation: Event log TCPIP	
Port: 49667/tcp	
UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[49667]	
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[49667]	
Port: 5504/tcp	
UUID: ed96b012-c8ce-4f60-a682-35535b12ff75, version 2	
Endpoint: ncacn_ip_tcp:192.168.1.1[5504]	
Port: 58889/tcp	
UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[58889]	
Annotation: Remote Fw APIs	
Port: 62067/tcp	
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0	
Endpoint: ncacn_http:192.168.1.1[62067]	
Annotation: RemoteAccessCheck	
UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1	
Endpoint: ncacn_http:192.168.1.1[62067]	
Named pipe : lsass	
Win32 service or process : Netlogon	
Description : Net Logon service	
UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0	
Endpoint: ncacn_http:192.168.1.1[62067]	
Named pipe : lsass	
Win32 service or process : lsass.exe	
Description : LSA access	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_http:192.168.1.1[62067]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_http:192.168.1.1[62067]	
...continues on next page...	

...continued from previous page...	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_http:192.168.1.1[62067]	
Annotation: KeyIso	
UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4	
Endpoint: ncacn_http:192.168.1.1[62067]	
Annotation: MS NT Directory DRS Interface	
Port: 62068/tcp	
UUID: 0b6edbf8-4a24-4fc6-8a23-942b1eca65d1, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[62068]	
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[62068]	
Named pipe : spoolss	
Win32 service or process : spoolsv.exe	
Description : Spooler service	
UUID: 4a452661-8290-4b36-8f8e-7f4093a94978, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[62068]	
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[62068]	
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[62068]	
Port: 62074/tcp	
UUID: 5b821720-f63b-11d0-aad2-00c04fc324db, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[62074]	
UUID: 6bffd098-a112-3610-9833-46c3f874532d, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[62074]	
Port: 62075/tcp	
UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[62075]	
Named pipe : lsass	
Win32 service or process : Netlogon	
Description : Net Logon service	
UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[62075]	
Annotation: Ngc Pop Key Service	
UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1	
Endpoint: ncacn_ip_tcp:192.168.1.1[62075]	
Annotation: Ngc Pop Key Service	
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2	
Endpoint: ncacn_ip_tcp:192.168.1.1[62075]	
Annotation: KeyIso	
Port: 62079/tcp	
UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5	
Endpoint: ncacn_ip_tcp:192.168.1.1[62079]	
Named pipe : dnsserver	
Win32 service or process : dns.exe	
Description : DNS Server	
...continues on next page...	

...continued from previous page...	
Port: 62102/tcp	UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1 Endpoint: ncacn_ip_tcp:192.168.1.1[62102] Annotation: Frs2 Service
Port: 62111/tcp	UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:192.168.1.1[62111]
Port: 62128/tcp	UUID: 3357951c-a1d1-47db-a278-ab945d063d03, version 1 Endpoint: ncacn_ip_tcp:192.168.1.1[62128]
Note: DCE/RPC or MSRPC services running on this host locally were identified. Reporting 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 information to gain more knowledge about the remote host and to conduct further attacks based on it.	
Solution: Solution type: Mitigation Filter incoming traffic to this ports.	
Affected Software/OS All systems exposing / disclosing information via DCE/RPC or MSRPC services.	
Vulnerability Insight DCE/RPC or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.	
Vulnerability Detection Method Reports previously collected (via 'DCE/RPC and MSRPC Services Enumeration' OID: 1.3.6.1.4.1.25623.1.0.108044) DCE/RPC or MSRPC services. This VT is reporting a severity by default. If the scanned network is e.g. a private LAN / private WAN which contains systems not accessible to the public (access restricted) and it is accepted that the service is disclosing information to this network please set the 'Network type' configuration of the following VT to e.g. 'Private LAN' or 'Private WAN': Global variable settings (OID: 1.3.6.1.4.1.25623.1.0.12288) In this case a 'Log' level result is used instead. Details: DCE/RPC and MSRPC Services Enumeration Reporting OID:1.3.6.1.4.1.25623.1.0.10736 Version used: 2025-11-26T05:40:08Z	

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

2.4.6 Medium 443/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired
Product detection result cpe:/a:ietf:transport_layer_security Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25 ↪623.1.0.103692)
Summary The remote server's SSL/TLS certificate has already expired.
Quality of Detection (QoD): 99%
Vulnerability Detection Result The certificate of the remote service expired on 2026-03-25 15:56:55. Certificate details: fingerprint (SHA-1) 5874345888B6F42D93AA793B86AF783F0A744882 fingerprint (SHA-256) 8FD86510D6D67A90EB9CE3FC13920356CEFDB704788610 ↪4EAB3B048DDBB9069D issued by CN=S-DC public key algorithm RSA public key size (bits) 2048 serial 7C6F8CE1170A83974B4A71DC0ED03453 signature algorithm sha256WithRSAEncryption subject CN=S-DC subject alternative names (SAN) None valid from 2025-09-23 15:56:55 UTC valid until 2026-03-25 15:56:55 UTC
Solution: Solution type: Mitigation Replace the SSL/TLS certificate by a new one.
Vulnerability Insight This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.
Vulnerability Detection Method Details: SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: 2026-03-13T05:54:58Z
Product Detection Result Product: cpe:/a:ietf:transport_layer_security ... continues on next page ...

...continued from previous page ...
Method: SSL/TLS: Collect and Report Certificate Details OID: 1.3.6.1.4.1.25623.1.0.103692)
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 resources supporting you with this task.
Affected Software/OS - All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols - CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder - CVE-2024-41270: Gorush v1.18.4 - CVE-2025-3200: Multiple products from Wiesemann & Theis
Vulnerability Insight The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: ... continues on next page ...

...continued from previous page ...
- 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 Checks 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: 2026-03-13T05:54:58Z
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 cve: CVE-2023-41928 cve: CVE-2024-41270 cve: CVE-2025-3200 url: https://ssl-config.mozilla.org url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html url: https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/0TLS-Protokoll/TLS-Protokoll_node.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch0eRichtlinien/TR03116/BSI-TR-03116-4.html url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters0-report-2014 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://certvde.com/en/advisories/VDE-2025-031/ url: https://gist.github.com/nyxfqq/cfae38fada582a0f576d154belaeb1fc url: https://advisories.ncsc.nl/advisory?id=NCSC-2024-0273 cert-bund: WID-SEC-2026-0180 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
...continues on next page ...

...continued from previous page ...

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

...continues on next page ...

...continued from previous page ...

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

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

2.4.7 Medium 17/tcp

Medium (CVSS: 5.0)
NVT: Check for Quote of the Day (qotd) Service (TCP)
Summary The Quote of the Day (qotd) service is running on this host.
Quality of Detection (QoD): 80%
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the network.
Solution: Solution type: Mitigation - Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry keys to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd Then launch cmd.exe and type : net stop simptcp net start simptcp To restart the service.
Vulnerability Insight A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote. Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.
Vulnerability Detection Method Details: Check for Quote of the Day (qotd) Service (TCP) OID:1.3.6.1.4.1.25623.1.0.10198 Version used: 2023-08-01T13:29:10Z
...
... continues on next page ...

...continued from previous page ...

References

cve: CVE-1999-0103

[\[return to 192.168.1.1 \]](#)**2.4.8 Medium 19/tcp**

Medium (CVSS: 5.0)

NVT: Check for Chargen Service (TCP)

Summary

The remote host is running a 'chargen' service.

Quality of Detection (QoD): 80%**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

An easy attack is 'ping-pong' in which an attacker spoofs a packet between two machines running chargen. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution:**Solution type:** Mitigation

- Under Unix systems, comment out the 'chargen' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\Simptcp\Parameters\EnableTcpChargen

HKLM\System\CurrentControlSet\Services\Simptcp\Parameters\EnableUdpChargen

Then launch cmd.exe and type :

net stop simptcp

net start simptcp

To restart the service.

Vulnerability Insight

When contacted, chargen responds with some random characters (something like all the characters in the alphabet in a row). When contacted via TCP, it will continue spewing characters until the client closes the connection.

The purpose of this service was to mostly to test the TCP/IP protocol by itself, to make sure that all the packets were arriving at their destination unaltered. It is unused these days, so it is suggested you disable it, as an attacker may use it to set up an attack against this host, or against a third party host using this host as a relay.

... continues on next page ...

...continued from previous page ...

Vulnerability Detection Method

Checks whether a chargen service is exposed on the target host.

Details: **Check for Chargen Service (TCP)**

OID:1.3.6.1.4.1.25623.1.0.10043

Version used: 2023-09-12T05:05:19Z

References

cve: CVE-1999-0103

cve: CVE-1999-0639

[\[return to 192.168.1.1 \]](#)**2.4.9 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: 4910081

Packet 2: 4911156

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.

... continues on next page ...

...continued from previous page ...
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 192.168.1.1](#)]

2.4.10 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:
... continues on next page ...

...continued from previous page ...
- 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

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

2.5 192.168.1.10

Host scan start Mon Apr 20 11:26:09 2026 UTC

Host scan end Mon Apr 20 11:34:43 2026 UTC

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

2.5.1 Medium 135/tcp

Medium (CVSS: 5.0)

NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary

... continues on next page ...

...continued from previous page...	
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC based service enumeration reporting.	
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: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:192.168.1.10[49664] Annotation: RemoteAccessCheck UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:192.168.1.10[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:192.168.1.10[49664] Annotation: Ngc Pop Key Service UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:192.168.1.10[49664] Annotation: Ngc Pop Key Service UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:192.168.1.10[49664] Annotation: KeyIso Port: 49665/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:192.168.1.10[49665] Port: 49666/tcp UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:192.168.1.10[49666] Annotation: Event log TCPIP Port: 49667/tcp UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1 Endpoint: ncacn_ip_tcp:192.168.1.10[49667] UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:192.168.1.10[49667] Port: 49668/tcp UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:192.168.1.10[49668] UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:192.168.1.10[49668] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1	
...continues on next page...	

...continued from previous page ... Endpoint: ncacn_ip_tcp:192.168.1.10[49668] UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:192.168.1.10[49668] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:192.168.1.10[49668] Port: 49669/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:192.168.1.10[49669] Annotation: RemoteAccessCheck Port: 49670/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:192.168.1.10[49670] Port: 49671/tcp UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1 Endpoint: ncacn_ip_tcp:192.168.1.10[49671] Annotation: Remote Fw APIs 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 information to gain more knowledge about the remote host and to conduct further attacks based on it.
Solution: Solution type: Mitigation Filter incoming traffic to this ports.
Affected Software/OS All systems exposing / disclosing information via DCE/RPC or MSRPC services.
Vulnerability Insight DCE/RPC or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.
Vulnerability Detection Method Reports previously collected (via 'DCE/RPC and MSRPC Services Enumeration' OID: 1.3.6.1.4.1.25623.1.0.108044) DCE/RPC or MSRPC services. This VT is reporting a severity by default. If the scanned network is e.g. a private LAN / private WAN which contains systems not accessible to the public (access restricted) and it is accepted that the service is disclosing information to this network please set the 'Network type' configuration of the following VT to e.g. 'Private LAN' or 'Private WAN': Global variable settings (OID: 1.3.6.1.4.1.25623.1.0.12288) In this case a 'Log' level result is used instead. Details: DCE/RPC and MSRPC Services Enumeration Reporting OID:1.3.6.1.4.1.25623.1.0.10736
... continues on next page ...

...continued from previous page ...

Version used: 2025-11-26T05:40:08Z

[\[return to 192.168.1.10 \]](#)

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

... continues on next page ...

...continued from previous page ...

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

[\[return to 192.168.1.10 \]](#)

This file was automatically generated.