

Scan Report

September 7, 2023

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 “ScanOpen_13_0”. The scan started at Thu Sep 7 19:58:13 2023 UTC and ended at . The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1	Result Overview	2
2	Results per Host	2
2.1	192.168.13.18	2
2.1.1	Medium 135/tcp	2
2.1.2	Low general/tcp	4
2.2	192.168.13.31	5
2.2.1	Medium 8000/tcp	6
2.2.2	Low general/tcp	7
2.2.3	Low general/icmp	8
2.3	192.168.13.25	9
2.3.1	Low general/tcp	9
2.4	192.168.13.1	10
2.4.1	Low general/icmp	10
2.4.2	Low general/tcp	11

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.13.18	0	1	1	0	0
192.168.13.31	0	1	2	0	0
192.168.13.25	0	0	1	0	0
192.168.13.1	0	0	2	0	0
Total: 4	0	2	6	0	0

Vendor security updates are not trusted.

Overrides are off. Even when a result has an override, this report uses the actual threat of the result.

Information on overrides is included in the report.

Notes are included in the report.

This report might not show details of all issues that were found.

Issues with the threat level “Log” are not shown.

Issues with the threat level “Debug” are not shown.

Issues with the threat level “False Positive” are not shown.

Only results with a minimum QoD of 70 are shown.

This report contains all 8 results selected by the filtering described above. Before filtering there were 118 results.

2 Results per Host

2.1 192.168.13.18

Host scan start Thu Sep 7 19:59:23 2023 UTC

Host scan end Thu Sep 7 20:12:11 2023 UTC

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

2.1.1 Medium 135/tcp

Medium (CVSS: 5.0)

NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary

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

... continues on next page ...

...continued from previous page...

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:192.168.13.18[49664]

Annotation: RemoteAccessCheck

UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1

Endpoint: ncacn_ip_tcp:192.168.13.18[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:192.168.13.18[49664]

Annotation: Ngc Pop Key Service

UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1

Endpoint: ncacn_ip_tcp:192.168.13.18[49664]

Annotation: Ngc Pop Key Service

UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2

Endpoint: ncacn_ip_tcp:192.168.13.18[49664]

Annotation: KeyIso

Port: 49665/tcp

UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1

Endpoint: ncacn_ip_tcp:192.168.13.18[49665]

Port: 49666/tcp

UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1

Endpoint: ncacn_ip_tcp:192.168.13.18[49666]

UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1

Endpoint: ncacn_ip_tcp:192.168.13.18[49666]

Port: 49667/tcp

UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1

Endpoint: ncacn_ip_tcp:192.168.13.18[49667]

Annotation: Windows Event Log

Port: 49668/tcp

UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1

Endpoint: ncacn_ip_tcp:192.168.13.18[49668]

Port: 49669/tcp

UUID: 0b6edbf8-4a24-4fc6-8a23-942b1eca65d1, version 1

Endpoint: ncacn_ip_tcp:192.168.13.18[49669]

UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1

Endpoint: ncacn_ip_tcp:192.168.13.18[49669]

Named pipe : spoolss

Win32 service or process : spoolsv.exe

Description : Spooler service

UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1

Endpoint: ncacn_ip_tcp:192.168.13.18[49669]

...continues on next page...

<p>...continued from previous page ...</p> <p>UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:192.168.13.18[49669] UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:192.168.13.18[49669] Port: 49670/tcp UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:192.168.13.18[49670] Annotation: RemoteAccessCheck UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1 Endpoint: ncacn_ip_tcp:192.168.13.18[49670] Annotation: Ngc Pop Key Service UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:192.168.13.18[49670] Annotation: Ngc Pop Key Service UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:192.168.13.18[49670] Annotation: KeyIso Port: 49678/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:192.168.13.18[49678] 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.</p>
<p>Impact An attacker may use this fact to gain more knowledge about the remote host.</p>
<p>Solution: Solution type: Mitigation Filter incoming traffic to this ports.</p>
<p>Vulnerability Detection Method Details: DCE/RPC and MSRPC Services Enumeration Reporting OID:1.3.6.1.4.1.25623.1.0.10736 Version used: 2022-06-03T10:17:07Z</p>

[\[return to 192.168.13.18 \]](#)

2.1.2 Low general/tcp

<p>Low (CVSS: 2.6) NVT: TCP Timestamps Information Disclosure</p>
<p>Summary The remote host implements TCP timestamps and therefore allows to compute the uptime. ... continues on next page ...</p>

...continued from previous page...
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: 195355476 Packet 2: 195356570
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: 2023-08-01T13:29:10Z
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

[[return to 192.168.13.18](#)]

2.2 192.168.13.31

Host scan start Thu Sep 7 19:59:23 2023 UTC
Host scan end Thu Sep 7 20:22:13 2023 UTC

Service (Port)	Threat Level
8000/tcp	Medium
general/tcp	Low
general/icmp	Low

2.2.1 Medium 8000/tcp

Medium (CVSS: 4.8) NVT: Cleartext Transmission of Sensitive Information via HTTP
<p>Summary The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.</p>
<p>Vulnerability Detection Result The following input fields were identified (URL:input name): http://192.168.13.31:8000/login/:password</p>
<p>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.</p>
<p>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.</p>
<p>Affected Software/OS Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.</p>
<p>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</p>
<p>References url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management ... continues on next page ...</p>

...continued from previous page ...

url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
 url: <https://cwe.mitre.org/data/definitions/319.html>

[[return to 192.168.13.31](#)]

2.2.2 Low general/tcp

Low (CVSS: 2.6) NVT: TCP Timestamps Information Disclosure
Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.
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: 367260738 Packet 2: 367261809
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: 2023-08-01T13:29:10Z
... continues on next page ...

...continued from previous page ...

References

url: <https://datatracker.ietf.org/doc/html/rfc1323>

url: <https://datatracker.ietf.org/doc/html/rfc7323>

url: <https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152>

[\[return to 192.168.13.31 \]](#)

2.2.3 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary

The remote host responded to an ICMP timestamp request.

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: 2023-05-11T09:09:33Z

... continues on next page ...

...continued from previous page ...

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

[\[return to 192.168.13.31 \]](#)**2.3 192.168.13.25**

Host scan start Thu Sep 7 19:59:23 2023 UTC

Host scan end

Service (Port)	Threat Level
general/tcp	Low

2.3.1 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

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: 75490240

Packet 2: 3967644957

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.

... continues on next page ...

...continued from previous page ...
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: 2023-08-01T13:29:10Z
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

[[return to 192.168.13.25](#)]

2.4 192.168.13.1

Host scan start Thu Sep 7 19:59:23 2023 UTC
Host scan end Thu Sep 7 20:37:03 2023 UTC

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

2.4.1 Low general/icmp

Low (CVSS: 2.1) NVT: ICMP Timestamp Reply Information Disclosure
Summary The remote host responded to an ICMP timestamp request.
Vulnerability Detection Result The following response / ICMP packet has been received: - ICMP Type: 14 - ICMP Code: 0
... continues on next page ...

...continued from previous page ...
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: 2023-05-11T09:09:33Z
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

[\[return to 192.168.13.1 \]](#)

2.4.2 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.
Vulnerability Detection Result It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: ...continues on next page ...

...continued from previous page...	
Packet 1: 618143878	
Packet 2: 618143986	
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: 2023-08-01T13:29:10Z	
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	

[[return to 192.168.13.1](#)]