Scan Report

August 10, 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 "My Computer". The scan started at Sun Aug 10 11:02:39 2025 UTC and ended at Sun Aug 10 11:15:42 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
192.168.0.107	1	1	1	0	0
Total: 1	1	1	1	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 3 results selected by the filtering described above. Before filtering there were 27 results.

1.1   Host Authentications

Host	Protocol	Result	Port/User
192.168.0.107	SMB	Success	Protocol SMB, Port 445, User

2   Results per Host

2.1   192.168.0.107

Host scan start   Sun Aug 10 11:03:10 2025 UTC
Host scan end   Sun Aug 10 11:15:36 2025 UTC

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

2.1.1   High 445/tcp

High (CVSS: 7.5)
NVT: Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability

Summary
Microsoft Windows is prone to an authentication bypass vulnerability via SMB/NETBIOS.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
`It was possible to login at the share 'IPC$' with an empty login and password.`

Impact
Successful exploitation could allow attackers to use shares to cause the system to crash.

Solution:
Solution type: Workaround
A workaround is to:
- Disable null session login
- Remove the share
- Enable passwords on the share

Affected Software/OS
- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows NT
- Microsoft Windows 2000
- Microsoft Windows in other implementations / versions might be affected as well

Vulnerability Insight
The flaw is due to an SMB share, allows full access to Guest users. If the Guest account is enabled, anyone can access the computer without a valid user account or password.

Vulnerability Detection Method
Send multiple crafted SMB requests to various shares and checks the responses.
Details: `Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability`
OID:`1.3.6.1.4.1.25623.1.0.801991`
Version used: `2025-04-16T05:39:43Z`

References
`cve: CVE-1999-0519`
`cve: CVE-1999-0520`
`cve: CVE-2002-1117`
`url: https://exchange.xforce.ibmcloud.com/vulnerabilities/1`
`url: https://exchange.xforce.ibmcloud.com/vulnerabilities/2`
`url: https://exchange.xforce.ibmcloud.com/vulnerabilities/3`
`url: https://exchange.xforce.ibmcloud.com/vulnerabilities/10093`
`url: https://seclab.cs.ucdavis.edu/projects/testing/vulner/36.html`

url: https://seclab.cs.ucdavis.edu/projects/testing/vulner/38.html

2.1.2   Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.107[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:192.168.0.107[49664]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.107[49664]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.0.107[49664]
     Annotation: KeyIso
Port: 49665/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.107[49665]
Port: 49666/tcp
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.107[49666]
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.107[49666]
Port: 49667/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.107[49667]
     Annotation: Windows Event Log
```

```
Port: 49668/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.107[49668]
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.107[49668]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.107[49668]
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.107[49668]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.107[49668]
Port: 49681/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.0.107[49681]
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

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

2.1.3   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: 4310790
Packet 2: 4312163
```

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 192.168.0.107]

This file was automatically generated.