

Scan Report

January 23, 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 “Scan with victim’s credentials”. The scan started at Fri Jan 23 09:31:10 2026 UTC and ended at Fri Jan 23 10:06:55 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
1.1	Host Authentications	2
2	Results per Host	2
2.1	192.168.57.20	2
2.1.1	High 445/tcp	2
2.1.2	High general/tcp	5
2.1.3	Medium 135/tcp	6
2.1.4	Low general/tcp	7

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.57.20	3	1	1	0	0
Total: 1	3	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 5 results selected by the filtering described above. Before filtering there were 27 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.57.20	SMB	Success	Protocol SMB, Port 445, User student

2 Results per Host

2.1 192.168.57.20

Host scan start Fri Jan 23 09:31:57 2026 UTC

Host scan end Fri Jan 23 10:06:52 2026 UTC

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

2.1.1 High 445/tcp

... continues on next page ...

... continued from previous page ...

High (CVSS: 10.0)

NVT: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS10-012.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service or bypass the authentication mechanism via brute force technique.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 7
- Microsoft Windows 2000 Service Pack and prior
- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows Vista Service Pack 2 and prior
- Microsoft Windows Server 2003 Service Pack 2 and prior
- Microsoft Windows Server 2008 Service Pack 2 and prior

Vulnerability Insight

- An input validation error exists while processing SMB requests and can be exploited to cause a buffer overflow via a specially crafted SMB packet.
- An error exists in the SMB implementation while parsing SMB packets during the Negotiate phase causing memory corruption via a specially crafted SMB packet.
- NULL pointer dereference error exists in SMB while verifying the 'share' and 'servername' fields in SMB packets causing denial of service.
- A lack of cryptographic entropy when the SMB server generates challenges during SMB NTLM authentication and can be exploited to bypass the authentication mechanism.

Vulnerability Detection Method

Details: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

OID:1.3.6.1.4.1.25623.1.0.902269

Version used: 2021-09-01T09:31:49Z

References

cve: CVE-2010-0020

cve: CVE-2010-0021

cve: CVE-2010-0022

cve: CVE-2010-0231

... continues on next page ...

... continued from previous page ...

```
url: http://support.microsoft.com/kb/971468
url: http://www.vupen.com/english/advisories/2010/0345
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms
→10-012
dfn-cert: DFN-CERT-2010-0192
```

High (CVSS: 8.1)

NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Service Pack 2

Vulnerability Insight

Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method

Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.

Details: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

OID:1.3.6.1.4.1.25623.1.0.810676

Version used: 2021-09-14T11:01:46Z

... continues on next page ...

<p>References</p> <p>cve: CVE-2017-0143 cve: CVE-2017-0144 cve: CVE-2017-0145 cve: CVE-2017-0146 cve: CVE-2017-0147 cve: CVE-2017-0148 bid: 96703 bid: 96704 bid: 96705 bid: 96707 bid: 96709 bid: 96706 url: https://support.microsoft.com/en-in/kb/4013078 url: https://technet.microsoft.com/library/security/MS17-010 url: https://github.com/rapid7/metasploit-framework/pull/8167/files cert-bund: CB-K17/0435 dfn-cert: DFN-CERT-2017-0448</p>	... continued from previous page ...
--	--------------------------------------

[[return to 192.168.57.20](#)]

2.1.2 High general/tcp

High (CVSS: 10.0)

NVT: OS End Of Life Detection

Product detection result

cpe:/o:microsoft:windows_7:-:-:
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↔.105937)

Summary

OS End Of Life Detection.

The Operating System on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result

The "Windows 7" Operating System on the remote host has reached the end of life.
CPE: cpe:/o:microsoft:windows_7:-:-:
EOL date: 2013-04-09
EOL info: <https://support.microsoft.com/en-us/lifecycle/search?sort=PN&alpha=Windows%207&Filter=FilterNO>

Solution:

Solution type: Mitigation

... continues on next page ...

<p>... continued from previous page ...</p> <p>Upgrade the Operating System on the remote host to a version which is still supported and receiving security updates by the vendor.</p> <p>Vulnerability Detection Method Details: OS End Of Life Detection OID:1.3.6.1.4.1.25623.1.0.103674 Version used: 2021-04-16T10:39:13Z</p> <p>Product Detection Result Product: cpe:/o:microsoft:windows_7:-:-: Method: OS Detection Consolidation and Reporting OID: 1.3.6.1.4.1.25623.1.0.105937)</p>

[[return to 192.168.57.20](#)]

2.1.3 Medium 135/tcp

<p>Medium (CVSS: 5.0) NVT: DCE/RPC and MSRPC Services Enumeration Reporting</p>
<p>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.</p> <p>Vulnerability Detection Result Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:</p> <pre> Port: 49152/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:192.168.57.20[49152] Port: 49153/tcp UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:192.168.57.20[49153] Annotation: Security Center UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:192.168.57.20[49153] Annotation: NRP server endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:192.168.57.20[49153] Annotation: DHCP Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:192.168.57.20[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 </pre> <p>... continues on next page ...</p>

<p>... continued from previous page ...</p> <pre> Endpoint: ncacn_ip_tcp:192.168.57.20[49153] Annotation: Event log TCPIP Port: 49154/tcp UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1 Endpoint: ncacn_ip_tcp:192.168.57.20[49154] Annotation: IP Transition Configuration endpoint UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1 Endpoint: ncacn_ip_tcp:192.168.57.20[49154] UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1 Endpoint: ncacn_ip_tcp:192.168.57.20[49154] Annotation: XactSrv service Port: 49155/tcp UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:192.168.57.20[49155] Port: 49157/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:192.168.57.20[49157] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access 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. </pre>
--

Annotation: Event log TCPIP

Port: 49154/tcp

UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1

Endpoint: ncacn_ip_tcp:192.168.57.20[49154]

Annotation: IP Transition Configuration endpoint

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

Endpoint: ncacn_ip_tcp:192.168.57.20[49154]

UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1

Endpoint: ncacn_ip_tcp:192.168.57.20[49154]

Annotation: XactSrv service

Port: 49155/tcp

UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2

Endpoint: ncacn_ip_tcp:192.168.57.20[49155]

Port: 49157/tcp

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

Endpoint: ncacn_ip_tcp:192.168.57.20[49157]

Named pipe : lsass

Win32 service or process : lsass.exe

Description : SAM access

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 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: 2017-06-13T07:06:12Z

[[return to 192.168.57.20](#)]

2.1.4 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP timestamps

Summary

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

... continues on next page ...

... 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: 287664

Packet 2: 287772

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

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: 2020-08-24T08:40:10Z

References

url: <http://www.ietf.org/rfc/rfc1323.txt>

url: <http://www.ietf.org/rfc/rfc7323.txt>

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

[[return to 192.168.57.20](#)]