Scan Report

February 22, 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 52.135.80.210”. The scan started at Fri Feb 21 23:44:02 2025 UTC and ended at Fri Feb 21 23:47:34 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
52.135.80.210	3	1	0	0	0
Total: 1	3	1	0	0	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
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.
It only lists hosts that produced issues.
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 4 results selected by the filtering described above. Before filtering there were 20 results.

2 Results per Host

2.1 52.135.80.210

Host scan start	Fri Feb 21 23:44:14 2025 UTC
Host scan end	Fri Feb 21 23:47:34 2025 UTC

Service (Port)	Threat Level
general/tcp	High
445/tcp	High
3389/tcp	High
135/tcp	Medium

2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: OS End Of Life Detection

Product detection result

```
cpe:/o:microsoft:windows_server_2003:-:sp2
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)
```

. . . continues on next page . . .

. . . continued from previous page . . .

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 Server 2003" Operating System on the remote host has reached the en
↪d of life.
CPE:               cpe:/o:microsoft:windows_server_2003:-:sp2
Installed version,
build or SP:       sp2
EOL date:          2015-07-14
EOL info:          https://support.microsoft.com/en-us/lifecycle/search?sort=PN&
↪alpha=Microsoft%20Windows%20Server%202003&Filter=FilterNO
```

Solution
Solution type: Mitigation

Vulnerability Detection Method
Details: `OS End Of Life Detection`
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: `$Revision: 8927 $`

Product Detection Result
Product: `cpe:/o:microsoft:windows_server_2003:-:sp2`
Method: `OS Detection Consolidation and Reporting`
OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 52.135.80.210]

2.1.2 High 445/tcp

High (CVSS: 9.3)
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.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: VendorFix

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

Affected Software/OS

Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition 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: `2019-05-03T10:54:50+0000`

References

```
CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147,
↪CVE-2017-0148
BID:96703, 96704, 96705, 96707, 96709, 96706
Other:
  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
```

[return to 52.135.80.210]

2.1.3 High 3389/tcp

High (CVSS: 9.3)

NVT: Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS12-020.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation could allow remote attackers to execute arbitrary code as the logged-on user or cause a denial of service condition.

Solution
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Windows 7 Service Pack 1 and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows 2K3 Service Pack 2 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior

Vulnerability Insight
The flaws are due to the way Remote Desktop Protocol accesses an object in memory that has been improperly initialized or has been deleted and the way RDP service processes the packets.

Vulnerability Detection Method
Details: `Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (267138.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.902818
Version used: `2019-05-03T12:31:27+0000`

References

```
CVE: CVE-2012-0002, CVE-2012-0152
BID:52353, 52354
Other:
  URL:http://blog.binaryninjas.org/?p=58
   URL:http://secunia.com/advisories/48395
   URL:http://support.microsoft.com/kb/2671387
   URL:http://www.securitytracker.com/id/1026790
   URL:http://technet.microsoft.com/en-us/security/bulletin/ms12-020
```

[return to 52.135.80.210]

2.1.4 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 p
↪rotocol:
Port: 1025/tcp
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:10.0.1.30[1025]
     Annotation: IPSec Policy agent endpoint
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:10.0.1.30[1025]
     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. 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: `$Revision: 6319 $`

[return to 52.135.80.210]