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 6.87.152.210”. The scan started at Sat Feb 22 08:28:46 2025 UTC and ended at Sat Feb 22 08:37:44 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
6.87.152.210	2	0	0	0	0
Total: 1	2	0	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 2 results selected by the filtering described above. Before filtering there were 15 results.

2 Results per Host

2.1 6.87.152.210

Host scan start	Sat Feb 22 08:28:57 2025 UTC
Host scan end	Sat Feb 22 08:37:44 2025 UTC

Service (Port)	Threat Level
445/tcp	High
general/tcp	High

2.1.1 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

. . . continues on next page . . .

. . . continued from previous page . . .

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 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 6.87.152.210]

2.1.2 High general/tcp

High (CVSS: 10.0)

NVT: OS End Of Life Detection

Product detection result

```
cpe:/o:microsoft:windows_xp
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 XP" Operating System on the remote host has reached the end of life
↪.
CPE:                cpe:/o:microsoft:windows_xp
EOL date:           2014-04-08
EOL info:           https://support.microsoft.com/en-us/lifecycle/search?sort=PN&
↪alpha=Microsoft%20Windows%20XP&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_xp`

Method: `OS Detection Consolidation and Reporting`

OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 6.87.152.210]

This file was automatically generated.