Scan Report

November 12, 2020

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 “FF-192.168.56.101”. The scan started at Thu Nov 12 08:52:09 2020 UTC and ended at Thu Nov 12 08:56:55 2020 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
192.168.56.101	4	0	0	0	0
Total: 1	4	0	0	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 4 results selected by the filtering described above. Before filtering there were 19 results.

1.1 Host Authentications

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

2 Results per Host

2.1 192.168.56.101

Host scan start Thu Nov 12 08:52:26 2020 UTC
Host scan end Thu Nov 12 08:56:17 2020 UTC

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

2.1.1 High 445/tcp

High (CVSS: 10.0)
NVT: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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

References
```
cve: CVE-2010-0020
cve: CVE-2010-0021
cve: CVE-2010-0022
cve: CVE-2010-0231
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: 10.0)
NVT: Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote

Summary

This host is missing a critical security update according to Microsoft Bulletin MS09-001.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation could allow remote unauthenticated attackers to cause denying the service by sending a specially crafted network message to a system running the server service.

Solution

Solution type: VendorFix

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

Affected Software/OS

- Microsoft Windows 2K Service Pack 4 and prior
- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows 2003 Service Pack 2 and prior

Vulnerability Insight

The issue is due to the way Server Message Block (SMB) Protocol software handles specially crafted SMB packets.

Vulnerability Detection Method

Details: `Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote`
OID:1.3.6.1.4.1.25623.1.0.900233

References

```
cve: CVE-2008-4114
cve: CVE-2008-4834
cve: CVE-2008-4835
bid: 31179
url: http://www.milw0rm.com/exploits/6463
url: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2009/ms
↪09-001
```

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.

. . . continues on next page . . .

... continued from previous page ...

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

References

```
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
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-0448
```

[return to 192.168.56.101]

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)
```

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
Upgrade the Operating System on the remote host to a version which is still supported and receiving security updates by the vendor.

Vulnerability Detection Method

Details: `OS End Of Life Detection`
OID:1.3.6.1.4.1.25623.1.0.103674

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 192.168.56.101]