Scan Report

October 9, 2017

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 "Windows (Slow and Very Deep Ultimate)". The scan started at Mon Oct 9 01:22:06 2017 UTC and ended at Mon Oct 9 01:31:19 2017 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
192.168.56.102	4	0	0	0	0
Total: 1	4	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 4 results selected by the filtering described above. Before filtering there were 20 results.

1.1 Host Authentications

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

2 Results per Host

2.1 192.168.56.102

Host scan start	Mon Oct 9 01:22:15 2017 UTC
Host scan end	Mon Oct 9 01:31:19 2017 UTC

Service (Port)	Threat Level
445/tcp	High

2.1.1 High 445/tcp

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.

. . . continues on next page . . .

... continued from previous page ...

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.
Impact Level: System/Network

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx

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
Version used: `$Revision: 5502 $`

References
`CVE: CVE-2008-4114, CVE-2008-4834, CVE-2008-4835`
`BID:31179`
`Other:`
`URL:http://www.milw0rm.com/exploits/6463`
`URL:http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx`

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

... continues on next page ...

... continued from previous page ...

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. Impact Level: System/Application

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx

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: `$Revision: 5437 $`

References
`CVE: CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0231`
`Other:`
`URL:http://secunia.com/advisories/38510/`
`URL:http://support.microsoft.com/kb/971468`
`URL:http://www.vupen.com/english/advisories/2010/0345`
`URL:http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx`

High (CVSS: 10.0)
NVT: Vulnerability in Server Service Could Allow Remote Code Execution (958644)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS08-067.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation could allow remote attackers to take complete control of an affected system. Impact Level: System
Variants of Conficker worm are based on the above described vulnerability. More details regarding the worm and means to resolve this can be found at, http://technet.microsoft.com/en-us/security/dd452420.aspx

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx

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
Flaw is due to an error in the Server Service, that does not properly handle specially crafted RPC requests.

Vulnerability Detection Method
Details:`Vulnerability in Server Service Could Allow Remote Code Execution (958644)`
OID:1.3.6.1.4.1.25623.1.0.900056
Version used: `$Revision: 5455 $`

References
```
CVE: CVE-2008-4250
BID:31874
Other:
  URL:http://secunia.com/advisories/32326
   URL:http://www.kb.cert.org/vuls/id/827267
   URL:http://xforce.iss.net/xforce/xfdb/46040
   URL:http://www.securitytracker.com/id?1021091
   URL:http://blogs.securiteam.com/index.php/archives/1150
   URL:http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx
```

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.
Impact Level: System

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS17-010

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: `$Revision: 6223 $`

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 192.168.56.102]