Scan Report

April 4, 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 "Windows XP". The scan started at and ended at . 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
192.168.100.82	4	1	0	0	0
Total: 1	4	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 5 results selected by the filtering described above. Before filtering there were 28 results.

2 Results per Host

2.1 192.168.100.82

Host scan start
Host scan end

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

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

Version used: `2019-10-21T09:55:06+0000`

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 192.168.100.82]

2.1.2 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.

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

. . . continues on next page . . .

. . . continued from previous page . . .

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
Version used: `2020-01-07T09:06:32+0000`

References

```
CVE: CVE-2008-4114, CVE-2008-4834, CVE-2008-4835
BID:31179
Other:
  URL:http://www.milw0rm.com/exploits/6463
   URL:https://docs.microsoft.com/en-us/security-updates/securitybulletins/2009/
↪ms09-001
```

High (CVSS: 10.0)
NVT: Microsoft Windows Server Service Remote Code Execution Vulnerability (921883)

Summary

This host is missing important security update according to Microsoft Bulletin MS06-040.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation could allow remote code execution by sending a specially crafted RPC request and can take complete control of an affected system.

Solution

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

Affected Software/OS

- Microsoft Windows XP Service Pack 2 and prior
- Microsoft Windows 2K3 Service Pack 1 and prior
- Microsoft Windows 2000 Service Pack 4 and prior

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight
The flaw is due to a boundary error in the 'CanonicalizePathName()' function in netapi32.dll and can be exploited to cause a stack-based buffer overflow via a malicious NetrpPathCanonicalize RPC request with an overly long path name to the Server Service.

Vulnerability Detection Method
Details: `Microsoft Windows Server Service Remote Code Execution Vulnerability (921883)`
OID:1.3.6.1.4.1.25623.1.0.902782
Version used: `2020-01-07T09:06:32+0000`

References

```
CVE: CVE-2006-3439
BID:19409
Other:
  URL:http://securitytracker.com/id?1016667
   URL:https://docs.microsoft.com/en-us/security-updates/securitybulletins/2006/
↪ms06-040
```

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.

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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `2019-12-20T12:42:55+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 192.168.100.82]

2.1.3 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.

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: 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1
     Endpoint: ncacn_ip_tcp:192.168.100.82[1025]
     UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1
     Endpoint: ncacn_ip_tcp:192.168.100.82[1025]
     Named pipe : atsvc
     Win32 service or process : mstask.exe
     Description : Scheduler service
     UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1
     Endpoint: ncacn_ip_tcp:192.168.100.82[1025]
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1
     Endpoint: ncacn_ip_tcp:192.168.100.82[1025]
     Annotation: Messenger Service
     Named pipe : ntsvcs
     Win32 service or process : messenger
     Description : Messenger service
Here is the list of DCE/RPC or MSRPC services running on this host via the UDP p
↪rotocol:
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 192.168.100.82]

This file was automatically generated.