Scan Report

June 11, 2021

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 "windowsxp". The scan started at Fri Jun 11 08:28:08 2021 UTC and ended at Fri Jun 11 08:31:30 2021 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
10.10.10.4 COMPUTER_1	2	0	0	14	0
Total: 1	2	0	0	14	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 "High" are not shown.
Issues with the threat level "Medium" are not shown.
Issues with the threat level "Low" are not shown.
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 16 results selected by the filtering described above. Before filtering there were 17 results.

2 Results per Host

2.1 10.10.10.4

Host scan start	Fri Jun 11 08:28:30 2021 UTC
Host scan end	Fri Jun 11 08:31:28 2021 UTC

Service (Port)	Threat Level
general/tcp	High
445/tcp	High
137/udp	Log
general/icmp	Log
general/tcp	Log
139/tcp	Log
445/tcp	Log
general/CPE-T	Log
135/tcp	Log
123/udp	Log

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)

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: 2021-04-16T10:39:13Z

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 10.10.10.4]

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.

. . . continues on next page . . .

... continued from previous page ...

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
- 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
Version used: `2020-06-04T12:11:49Z`

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`

... continues on next page ...

... continued from previous page ...

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

[return to 10.10.10.4]

2.1.3 Log 137/udp

Log (CVSS: 0.0)
NVT: Using NetBIOS to retrieve information from a SMB host

Summary
This script is using NetBIOS (port UDP:137) to retrieve information from a SMB host.

Vulnerability Detection Result

```
The following 6 NetBIOS names have been gathered :
 COMPUTER_1      = Computer name
 COMPUTER_1      = This is the computer name registered for workstation services
↪ by a WINS client.
 WORKGROUP       = Workgroup / Domain name
 WORKGROUP       = Workgroup / Domain name (part of the Browser elections)
The remote host has the following MAC address on its adapter :
 08:00:27:7b:f5:ac
If you do not want to allow everyone to find the NetBIOS name of your computer,
↪you should filter incoming traffic to this port.
```

Solution:

Log Method
Details: Using NetBIOS to retrieve information from a SMB host
OID:1.3.6.1.4.1.25623.1.0.10150
Version used: 2021-04-15T13:23:31Z

[return to 10.10.10.4]

2.1.4 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

... continues on next page ...

... continued from previous page ...

Summary
The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Solution:

Log Method
Details: `ICMP Timestamp Detection`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2021-03-23T06:51:29Z`

References
`cve: CVE-1999-0524`
`url: http://www.ietf.org/rfc/rfc0792.txt`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 10.10.10.4]

2.1.5 Log general/tcp

Log (CVSS: 0.0)
NVT: Hostname Determination Reporting

Summary
The script reports information on how the hostname of the target was determined.

Vulnerability Detection Result
`Hostname determination for IP 10.10.10.4:`
`Hostname|Source`
`10.10.10.4|IP-address`

Solution:

Log Method
Details: `Hostname Determination Reporting`
OID:1.3.6.1.4.1.25623.1.0.108449

... continues on next page ...

... continued from previous page ...

Version used: 2018-11-19T11:11:31Z

Log (CVSS: 0.0)
NVT: Traceroute

Summary
Collect information about the network route and network distance between the scanner host and the target host.

Vulnerability Detection Result
```
Network route from scanner (10.10.10.3) to target (10.10.10.4):
10.10.10.3
10.10.10.4
Network distance between scanner and target: 2
```

Solution:

Vulnerability Insight
For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.

Log Method
A combination of the protocols ICMP and TCP is used to determine the route. This method is applicable for IPv4 only and it is also known as 'traceroute'.
Details: Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: 2021-03-12T14:25:59Z

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several VTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

Vulnerability Detection Result
```
Best matching OS:
OS:           Windows XP
CPE:          cpe:/o:microsoft:windows_xp
Found by NVT: 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)
```

... continues on next page ...

... continued from previous page ...

```
Concluded from SMB/Samba banner on port 445/tcp:
OS String:  Windows 5.1
SMB String: Windows 2000 LAN Manager
Setting key "Host/runs_windows" based on this information
Other OS detections (in order of reliability):
OS:           Microsoft Windows
CPE:          cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.108044 (DCE/RPC and MSRPC Services Enumerati
↪on)
Concluded from DCE/RPC and MSRPC Services Enumeration on port 135/tcp
OS:           Microsoft Windows
CPE:          cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.10150 (Using NetBIOS to retrieve information
↪ from a SMB host)
Concluded from NetBIOS information on port 137/udp
```

Solution:

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2021-05-17T10:34:03Z

References
url: https://community.greenbone.net/c/vulnerability-tests

[return to 10.10.10.4]

2.1.6 Log 139/tcp

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary
This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Vulnerability Detection Result
A SMB server is running on this port

Solution:

Log Method
Details: SMB/CIFS Server Detection

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.11011
Version used: 2020-11-10T15:30:28Z

[return to 10.10.10.4]

2.1.7 Log 445/tcp

Log (CVSS: 0.0)
NVT: Microsoft SMB Signing Disabled

Summary
Checks if SMB Signing is disabled at the remote SMB server.

Vulnerability Detection Result
SMB Signing is disabled at the server.

Solution:

Log Method
Details: Microsoft SMB Signing Disabled
OID:1.3.6.1.4.1.25623.1.0.802726
Version used: 2020-12-07T08:53:10Z

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

Summary
It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Vulnerability Detection Result
Detected SMB workgroup: WORKGROUP
Detected SMB server: Windows 2000 LAN Manager
Detected OS: Windows 5.1

Solution:

Log Method
Details: SMB NativeLanMan
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: 2021-04-15T13:23:31Z

Log (CVSS: 0.0)
NVT: SMB Remote Version Detection

Summary
Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.

Vulnerability Detection Result
`Only SMBv1 is enabled on remote target`

Solution:

Log Method
Details: `SMB Remote Version Detection`
OID:1.3.6.1.4.1.25623.1.0.807830
Version used: `2019-05-16T07:13:31Z`

Log (CVSS: 0.0)
NVT: SMBv1 enabled (Remote Check)

Summary
The host has enabled SMBv1 for the SMB Server.

Vulnerability Detection Result
`SMBv1 is enabled for the SMB Server`

Solution:

Log Method
Checks if SMBv1 is enabled for the SMB Server based on the information provided by the following VT:
- SMB Remote Version Detection (OID: 1.3.6.1.4.1.25623.1.0.807830).
Details: `SMBv1 enabled (Remote Check)`
OID:1.3.6.1.4.1.25623.1.0.140151
Version used: `2021-03-19T08:40:35Z`

References
`url: https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-`
`↪Practices`
`url: https://support.microsoft.com/en-us/kb/2696547`
`url: https://support.microsoft.com/en-us/kb/204279`

Log (CVSS: 0.0) NVT: SMB/CIFS Server Detection
Summary This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.
Vulnerability Detection Result `A CIFS server is running on this port`
Solution:
Log Method Details: `SMB/CIFS Server Detection` OID:1.3.6.1.4.1.25623.1.0.11011 Version used: `2020-11-10T15:30:28Z`

[return to 10.10.10.4]

2.1.8 Log general/CPE-T

Log (CVSS: 0.0) NVT: CPE Inventory
Summary This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan. Note: Some CPEs for specific products might show up twice or more in the output. Background: After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.
Vulnerability Detection Result `10.10.10.4|cpe:/o:microsoft:windows_xp`
Solution:
Log Method Details: `CPE Inventory` OID:1.3.6.1.4.1.25623.1.0.810002 Version used: `2021-04-16T10:39:13Z`
References `url: https://nvd.nist.gov/products/cpe`

[return to 10.10.10.4]

2.1.9 Log 135/tcp

Log (CVSS: 0.0) NVT: DCE/RPC and MSRPC Services Enumeration
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. The actual reporting takes place in the NVT 'DCE/RPC and MSRPC Services Enumeration Reporting' (OID: 1.3.6.1.4.1.25623.1.0.10736)
Vulnerability Detection Result `A DCE endpoint resolution service seems to be running on this port.`
Impact An attacker may use this fact to gain more knowledge about the remote host.
Solution: **Solution type:** Mitigation Filter incoming traffic to this port.
Log Method Details: `DCE/RPC and MSRPC Services Enumeration` OID:1.3.6.1.4.1.25623.1.0.108044 Version used: `2021-04-15T13:23:31Z`

[return to 10.10.10.4]

2.1.10 Log 123/udp

Log (CVSS: 0.0) NVT: NTP(d) Server Detection
Summary This script performs detection of NTP servers.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution: Quickfix: Restrict default access to ignore all info packets.
. . . continues on next page . . .

... continued from previous page ...

Vulnerability Insight
It is possible to determine a lot of information about the remote host by querying the NTP (Network Time Protocol) variables - these include OS descriptor, and time settings.

Log Method
Details: `NTP(d) Server Detection`
OID:1.3.6.1.4.1.25623.1.0.10884
Version used: `2020-11-10T15:30:28Z`

[return to 10.10.10.4]