Scan Report

May 2, 2018

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 172.30.6.41". The scan started at Mon Apr 30 03:41:54 2018 UTC and ended at Mon Apr 30 04:09:05 2018 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
172.30.6.41 mcgl-20002870.comviva.com	1	0	0	8	0
Total: 1	1	0	0	8	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
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 "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.

This report contains all 9 results selected by the filtering described above. Before filtering there were 11 results.

2 Results per Host

2.1 172.30.6.41

Host scan start	Mon Apr 30 03:42:54 2018 UTC
Host scan end	Mon Apr 30 04:09:05 2018 UTC

Service (Port)	Threat Level
general/tcp	High
general/tcp	Log
general/CPE-T	Log
general/SMBClient	Log
135/tcp	Log
445/tcp	Log

2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: OS End Of Life Detection

Product detection result
`cpe:/o:microsoft:windows_10:1511`
`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 10" Operating System on the remote host has reached the end of life
↪.
CPE:                cpe:/o:microsoft:windows_10:1511
Installed version,
build or SP:        1511
EOL date:           2017-10-10
EOL info:           https://support.microsoft.com/en-US/help/13853/windows-lifecy
↪cle-fact-sheet
```

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_10:1511`
Method: `OS Detection Consolidation and Reporting`
OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 172.30.6.41]

2.1.2 Log general/tcp

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

Summary
This script consolidates the OS information detected by several NVTs 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 openvas-plugins@wald.intevation.org.

Vulnerability Detection Result
```
Best matching OS:
```

... continues on next page ...

... continued from previous page ...

```
OS: Windows 10 Pro 10586
CPE: cpe:/o:microsoft:windows_10:1511
Found by NVT: 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)
Concluded from SMB/Samba banner on port 445/tcp: OS String: Windows 10 Pro 10586
↪; SMB String: Windows 10 Pro 6.3
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
```

Log Method
Details:`OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `$Revision: 9462 $`

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result

```
Here is the route from 192.168.74.128 to 172.30.6.41:
192.168.74.128
172.30.6.41
```

Solution
Block unwanted packets from escaping your network.

Log Method
Details:`Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `$Revision: 8528 $`

[return to 172.30.6.41]

2.1.3 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.

Vulnerability Detection Result
`172.30.6.41|cpe:/o:microsoft:windows_10:1511`

Log Method
Details:`CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `$Revision: 8140 $`

[return to 172.30.6.41]

2.1.4 Log general/SMBClient

Log (CVSS: 0.0)
NVT: SMB Test with 'smbclient'

Summary
This script tests the remote host SMB Functions with the 'smbclient' tool.

Vulnerability Detection Result
```
The tool "smbclient" is not available for OpenVAS.
Therefore none of the tests using smbclient are executed.
```

Log Method
Details:`SMB Test with 'smbclient'`
OID:1.3.6.1.4.1.25623.1.0.90011
Version used: `$Revision: 6841 $`

[return to 172.30.6.41]

2.1.5 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.

... continues on next page ...

... continued from previous page ...

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: `$Revision: 8145 $`

[return to 172.30.6.41]

2.1.6 Log 445/tcp

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: COMVIVA
Detected SMB server: Windows 10 Pro 6.3
Detected OS: Windows 10 Pro 10586
```

Log Method
Details:`SMB NativeLanMan`
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: `$Revision: 9485 $`

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

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

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Result
`A CIFS server is running on this port`

Log Method
Details:`SMB/CIFS Server Detection`
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: `$Revision: 9608 $`

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
`SMBv1 and SMBv2 are enabled on remote target`

Log Method
Details:`SMB Remote Version Detection`
OID:1.3.6.1.4.1.25623.1.0.807830
Version used: `$Revision: 5438 $`

[return to 172.30.6.41]