Scan Report

April 7, 2024

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 “Windows2000 Scan”. The scan started at Sat Mar 30 03:08:50 2024 UTC and ended at Sat Mar 30 03:18:18 2024 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
172.16.36.131 WINWORLD-2KWS	3	1	1	0	0
Total: 1	3	1	1	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 5 results selected by the filtering described above. Before filtering there were 19 results.

2 Results per Host

2.1 172.16.36.131

Host scan start	Sat Mar 30 03:10:18 2024 UTC
Host scan end	Sat Mar 30 03:18:13 2024 UTC

Service (Port)	Threat Level
general/tcp	High
445/tcp	High
135/tcp	Medium
general/icmp	Low

2.1.1 High general/tcp

High (CVSS: 10.0)

NVT: Operating System (OS) End of Life (EOL) Detection

Product detection result

```
cpe:/o:microsoft:windows_2000
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪.105937)
```

Summary
The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

Quality of Detection: 80

Vulnerability Detection Result

```
The "Windows 2000" Operating System on the remote host has reached the end of li
↪fe.
CPE:                cpe:/o:microsoft:windows_2000
EOL date:           2010-07-13
EOL info:           https://support.microsoft.com/en-us/lifecycle/search/default.
↪aspx?sort=PN&alpha=Windows+2000&Filter=FilterNO
```

Impact
An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:
Solution type: Mitigation
Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

Vulnerability Detection Method
Checks if an EOL version of an OS is present on the target host.
Details: `Operating System (OS) End of Life (EOL) Detection`
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: `2024-02-28T14:37:42Z`

Product Detection Result
Product: `cpe:/o:microsoft:windows_2000`
Method: `OS Detection Consolidation and Reporting`
OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 172.16.36.131]

2.1.2 High 445/tcp

High (CVSS: 10.0)

NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Quality of Detection: 99

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
administrator:
```

Solution:
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2024-02-09T14:47:30Z`

References

```
cve: CVE-1999-0503
cve: CVE-1999-0504
cve: CVE-1999-0505
cve: CVE-1999-0506
cve: CVE-2000-0222
cve: CVE-2005-3595
```

High (CVSS: 8.1)

NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Quality of Detection: 95

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 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: `2023-07-14T16:09:27Z`

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
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/4013078
url: http://www.securityfocus.com/bid/96703
url: http://www.securityfocus.com/bid/96704
url: http://www.securityfocus.com/bid/96705
url: http://www.securityfocus.com/bid/96707
url: http://www.securityfocus.com/bid/96709
url: http://www.securityfocus.com/bid/96706
url: https://technet.microsoft.com/library/security/MS17-010
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://github.com/rapid7/metasploit-framework/pull/8167/files
cert-bund: CB-K17/0435
dfn-cert: DFN-CERT-2017-0448
```

[return to 172.16.36.131]

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.

Quality of Detection: 80

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: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1
     Endpoint: ncacn_ip_tcp:172.16.36.131[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:172.16.36.131[1025]
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

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2022-06-03T10:17:07Z`

[return to 172.16.36.131]

2.1.4 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

Vulnerability Detection Result

```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
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.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 172.16.36.131]

This file was automatically generated.