Scan Report

November 20, 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 192.168.1.5". The scan started at Tue Nov 20 22:35:16 2018 UTC and ended at Tue Nov 20 22:38:30 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
192.168.1.5	1	1	1	0	0
Total: 1	1	1	1	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 3 results selected by the filtering described above. Before filtering there were 14 results.

2 Results per Host

2.1 192.168.1.5

Host scan start	Tue Nov 20 22:35:26 2018 UTC
Host scan end	Tue Nov 20 22:38:30 2018 UTC

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

2.1.1 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.

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.

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory

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: 11874 $`

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 192.168.1.5]

2.1.2 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary

... continues on next page ...

... continued from previous page ...

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: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.5[49152]
Port: 49153/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.5[49153]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
Port: 49154/tcp
     UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.5[49154]
     Annotation: Security Center
     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.5[49154]
     Annotation: NRP server endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.5[49154]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.5[49154]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.5[49154]
     Annotation: Event log TCPIP
Port: 49155/tcp
     UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.5[49155]
     Annotation: AppInfo
     UUID: 2eb08e3e-639f-4fba-97b1-14f878961076, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.5[49155]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.5[49155]
     Annotation: IP Transition Configuration endpoint
     UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.5[49155]
     Annotation: AppInfo
     UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.5[49155]
     Annotation: AppInfo
```

... continues on next page ...

... continued from previous page ...

```
      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.5[49155]
      UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.5[49155]
      Annotation: XactSrv service
      UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.5[49155]
      Annotation: IKE/Authip API
      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.5[49155]
      Annotation: Impl friendly name
      UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.5[49155]
      Annotation: AppInfo
Port: 49156/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:192.168.1.5[49156]
Port: 49158/tcp
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.5[49158]
      Annotation: IPSec Policy agent endpoint
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.5[49158]
      Annotation: Remote Fw APIs
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 192.168.1.5]

2.1.3 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 28655
Packet 2: 28765
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `$Revision: 10411 $`

References
```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
```

[return to 192.168.1.5]