Summary

This document reports on the results of an automatic security scan. 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.

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 23 results.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Scan started:	**Fri Oct 24 20:04:36 2021 UTC**
Scan ended:	Fri Oct 24 20:21:02 2021 UTC
Task:	Blue

Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
10.10.148.71	Oct 24, 20:04:46	Oct 24, 20:21:02	1	3	1	0	0
Total: 1			1	3	1	0	0

Results per Host

Host 10.10.148.71

Scanning of this host started at:	Sun Feb 28 00:04:46 2021 UTC
Number of results:	5

Port Summary for Host 10.10.148.71

Service (Port)	Threat Level
3389/tcp	Medium
135/tcp	Medium
general/tcp	Low
445/tcp	High

Security Issues for Host 10.10.148.71

High (CVSS: 9.3) 445/tcp

NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676)

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

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
CERT:	CB-K17/0435, DFN-CERT-2017-0448
Other:	https://support.microsoft.com/en-in/kb/4013078
	https://technet.microsoft.com/library/security/MS17-010
	https://github.com/rapid7/metasploit-framework/pull/8167/files

Medium (CVSS: 5.0) 135/tcp

NVT: DCE/RPC and MSRPC Services Enumeration Reporting (OID: 1.3.6.1.4.1.25623.1.0.10736)

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 protocol:

Port: 49152/tcp

     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:10.10.148.71[49152]

Port: 49153/tcp

     UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1
```

```
     Endpoint: ncacn_ip_tcp:10.10.148.71[49153]
     Annotation: Security Center

     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
     Endpoint: ncacn_ip_tcp:10.10.148.71[49153]
     Annotation: NRP server endpoint

     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:10.10.148.71[49153]
     Annotation: DHCP Client LRPC Endpoint

     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:10.10.148.71[49153]
     Annotation: DHCPv6 Client LRPC Endpoint

     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:10.10.148.71[49153]
     Annotation: Event log TCPIP

Port: 49154/tcp

     UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
     Endpoint: ncacn_ip_tcp:10.10.148.71[49154]

     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:10.10.148.71[49154]
     Annotation: IP Transition Configuration endpoint

     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:10.10.148.71[49154]

     UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
     Endpoint: ncacn_ip_tcp:10.10.148.71[49154]
     Annotation: XactSrv service

     UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
     Endpoint: ncacn_ip_tcp:10.10.148.71[49154]
     Annotation: IKE/Authip API

     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:10.10.148.71[49154]
     Annotation: Impl friendly name

Port: 49158/tcp

     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:10.10.148.71[49158]

Port: 49160/tcp

     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:10.10.148.71[49160]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access

Note: DCE/RPC or MSRPC services running on this host locally were identified. Reporting 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 $

Medium (CVSS: 4.3) 3389/tcp
NVT: SSL/TLS: Report Weak Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.103440)

Summary

This routine reports all Weak SSL/TLS cipher suites accepted by a service.

NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result

```
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
```

Solution

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

Please see the references for more resources supporting you with this task.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength:

- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).

- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).

- 1024 bit RSA authentication is considered to be insecure and therefore as weak.

- Any cipher considered to be secure for only the next 10 years is considered as medium

- Any other cipher is considered as strong

Vulnerability Detection Method

Details: SSL/TLS: Report Weak Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.103440)

Version used: $Revision: 11135 $

References

CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000

CERT: CB-K17/1750, CB-K16/1593, CB-K16/1552, CB-K16/1102, CB-K16/0617, CB-K16/0599, CB-K16/0168, CB-K16/0121, CB-K16/0090, CB-K16/0030, CB-K15/1751, CB-K15/1591, CB-K15/1550, CB-K15/1517, CB-K15/1514, CB-K15/1464, CB-K15/1442, CB-K15/1334, CB-K15/1269, CB-K15/1136, CB-K15/1090, CB-K15/1059, CB-K15/1022, CB-K15/1015, CB-K15/0986, CB-K15/0964, CB-K15/0962, CB-K15/0932, CB-K15/0927, CB-K15/0926, CB-K15/0907, CB-K15/0901, CB-K15/0896, CB-K15/0889, CB-K15/0877, CB-K15/0850, CB-K15/0849, CB-K15/0834, CB-K15/0827, CB-K15/0802, CB-K15/0764, CB-K15/0733, CB-K15/0667, CB-K14/0935, CB-K13/0942, DFN-CERT-2017-1821, DFN-CERT-2016-1692, DFN-CERT-2016-

1648, DFN-CERT-2016-1168, DFN-CERT-2016-0665, DFN-CERT-2016-0642, DFN-CERT-2016-0184, DFN-CERT-2016-0135, DFN-CERT-2016-0101, DFN-CERT-2016-0035, DFN-CERT-2015-1853, DFN-CERT-2015-1679, DFN-CERT-2015-1632, DFN-CERT-2015-1608, DFN-CERT-2015-1542, DFN-CERT-2015-1518, DFN-CERT-2015-1406, DFN-CERT-2015-1341, DFN-CERT-2015-1194, DFN-CERT-2015-1144, DFN-CERT-2015-1113, DFN-CERT-2015-1078, DFN-CERT-2015-1067, DFN-CERT-2015-1038, DFN-CERT-2015-1016, DFN-CERT-2015-1012, DFN-CERT-2015-0980, DFN-CERT-2015-0977, DFN-CERT-2015-0976, DFN-CERT-2015-0960, DFN-CERT-2015-0956, DFN-CERT-2015-0944, DFN-CERT-2015-0937, DFN-CERT-2015-0925, DFN-CERT-2015-0884, DFN-CERT-2015-0881, DFN-CERT-2015-0879, DFN-CERT-2015-0866, DFN-CERT-2015-0844, DFN-CERT-2015-0800, DFN-CERT-2015-0737, DFN-CERT-2015-0696, DFN-CERT-2014-0977

Other: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html

https://bettercrypto.org/

https://mozilla.github.io/server-side-tls/ssl-config-generator/

Medium (CVSS: 4.0) 3389/tcp

NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm (OID: 1.3.6.1.4.1.25623.1.0.105880)

Summary

The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure signature algorithms:

Subject:               CN=Jon-PC
Signature Algorithm:   sha1WithRSAEncryption
```

Solution

Solution type: Mitigation

Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:

- Secure Hash Algorithm 1 (SHA-1)

- Message Digest 5 (MD5)

- Message Digest 4 (MD4)

- Message Digest 2 (MD2)

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.

NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:

Fingerprint1

or

fingerprint1,Fingerprint2

Vulnerability Detection Method

Check which hashing algorithm was used to sign the remote SSL/TLS certificate.

Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm (OID: 1.3.6.1.4.1.25623.1.0.105880)

Version used: $Revision: 11524 $

References

Other: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

Low (CVSS: 2.6) general/tcp
NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

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: 41539
Packet 2: 41668
```

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 the references for more information.

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: 14310 $

References

Other: http://www.ietf.org/rfc/rfc1323.txt
http://www.microsoft.com/en-us/download/details.aspx?id=9152

This file was automatically generated.