OpenVas Vulnerability Report

HackerTarget.com hosts a suite of **trusted open source** vulnerability scanners. Secure your Attack Surface with our vulnerability discovery and network intelligence solutions.

This report was autogenerated using the open source OpenVAS Vulnerability Scanner.

Table of Contents

Summary

Scan started: **Tue Feb 12 11:08:49 2019 UTC**
Scan ended: Tue Feb 12 11:18:44 2019 UTC

1	6	1
HIGH	MEDIUM	LOW

Any **HIGH** and **MEDIUM** severity vulnerabilities should be investigated and confirmed so that remediation can take place. **LOW** risk items should not be ignored as they can be chained with other vulnerabilities to enable further attacks.

Host Summary

Host	Start	End	High	Medium	Low	Log
192.168.1.56 (WIDGETServer)	Feb 12, 11:09	Feb 12, 11:18	1	6	1	0
Total: 1			1	6	1	0

Vulnerability Summary

Severity	Description	CVSS	Count
High	Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3	1
Medium	DCE/RPC and MSRPC Services Enumeration Reporting	5.0	1
Medium	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5.0	1
Medium	SSL/TLS: Report Weak Cipher Suites	4.3	4
Low	TCP timestamps	2.6	1

Results by Host

Host 192.168.1.56

Host scan started: Tue Feb 12 11:09:04 2019 UTC

Port Summary for Host 192.168.1.56

Service (Port)	Severity
general/tcp	Low
3389/tcp	Medium
636/tcp	Medium
445/tcp	High
443/tcp	Medium
135/tcp	Medium
3269/tcp	Medium

Security Issues for Host 192.168.1.56

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: 49664/tcp

UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49664]

Port: 49665/tcp

UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49665]
Annotation: DHCP Client LRPC Endpoint

UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49665]
Annotation: DHCPv6 Client LRPC Endpoint

UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49665]
Annotation: Event log TCPIP

Port: 49666/tcp

UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
Endpoint: ncacn_ip_tcp:192.168.1.56[49666]
Annotation: RemoteAccessCheck

UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49666]
Named pipe : lsass
Win32 service or process : Netlogon
Description : Net Logon service

UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
Endpoint: ncacn_ip_tcp:192.168.1.56[49666]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : LSA access

UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49666]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : SAM access

UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49666]
Annotation: Ngc Pop Key Service

UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49666]
Annotation: Ngc Pop Key Service

UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
Endpoint: ncacn_ip_tcp:192.168.1.56[49666]
Annotation: KeyIso

UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49666]
Annotation: Impl friendly name

UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
Endpoint: ncacn_ip_tcp:192.168.1.56[49666]
Annotation: MS NT Directory DRS Interface

Port: 49668/tcp

UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]
Annotation: UserMgrCli

UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]
Named pipe : atsvc
Win32 service or process : mstask.exe
Description : Scheduler service

UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]
Annotation: AppInfo

UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]

UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]
Annotation: Proxy Manager provider server endpoint

UUID: 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]

UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]

UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]

UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]
Annotation: IP Transition Configuration endpoint

UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]
Annotation: AppInfo

UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]
Annotation: AppInfo

UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]

UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]
Annotation: UserMgrCli

UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]
Annotation: Proxy Manager client server endpoint

UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]
Annotation: Adh APIs

UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]

UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]
Annotation: AppInfo

UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49668]
Annotation: AppInfo

Port: 49673/tcp

UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
Endpoint: ncacn_http:192.168.1.56[49673]
Annotation: RemoteAccessCheck

UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
Endpoint: ncacn_http:192.168.1.56[49673]
Named pipe : lsass
Win32 service or process : Netlogon
Description : Net Logon service

UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
Endpoint: ncacn_http:192.168.1.56[49673]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : LSA access

UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
Endpoint: ncacn_http:192.168.1.56[49673]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : SAM access

UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
Endpoint: ncacn_http:192.168.1.56[49673]
Annotation: Ngc Pop Key Service

UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
Endpoint: ncacn_http:192.168.1.56[49673]
Annotation: Ngc Pop Key Service

UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
Endpoint: ncacn_http:192.168.1.56[49673]
Annotation: KeyIso

UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
Endpoint: ncacn_http:192.168.1.56[49673]
Annotation: MS NT Directory DRS Interface

Port: 49674/tcp

UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
Endpoint: ncacn_ip_tcp:192.168.1.56[49674]
Annotation: RemoteAccessCheck

UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49674]
Named pipe : lsass
Win32 service or process : Netlogon
Description : Net Logon service

UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
Endpoint: ncacn_ip_tcp:192.168.1.56[49674]
Named pipe : lsass
Win32 service or process : lsass.exe

Description : LSA access

UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49674]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : SAM access

UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49674]
Annotation: Ngc Pop Key Service

UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49674]
Annotation: Ngc Pop Key Service

UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
Endpoint: ncacn_ip_tcp:192.168.1.56[49674]
Annotation: KeyIso

Port: 49675/tcp

UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49675]

UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49675]
Named pipe : spoolss
Win32 service or process : spoolsv.exe
Description : Spooler service

UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49675]

UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49675]

UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49675]

Port: 49683/tcp

UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
Endpoint: ncacn_ip_tcp:192.168.1.56[49683]

Port: 49728/tcp

UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5
Endpoint: ncacn_ip_tcp:192.168.1.56[49728]
Named pipe : dnsserver
Win32 service or process : dns.exe
Description : DNS Server

Port: 49914/tcp

UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1
Endpoint: ncacn_ip_tcp:192.168.1.56[49914]
Annotation: Frs2 Service

Port: 63520/tcp

UUID: 91ae6020-9e3c-11cf-8d7c-00aa00c091be, version 0
Endpoint: ncacn_ip_tcp:192.168.1.56[63520]
Named pipe : cert
Win32 service or process : certsrv.exe
Description : Certificate service

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: 5.0) 443/tcp
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS (OID: 1.3.6.1.4.1.25623.1.0.108031)

Summary

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result

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

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Solution

Solution type: Mitigation

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

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

Affected Software/OS

Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight

These rules are applied for the evaluation of the vulnerable cipher suites:

- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method

Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS (OID: 1.3.6.1.4.1.25623.1.0.108031)

Version used: $Revision: 5232 $

References

CVE: CVE-2016-2183, CVE-2016-6329

CERT: CB-K18/0296, CB-K17/1980, CB-K17/1871, CB-K17/1803, CB-K17/1753, CB-K17/1750, CB-K17/1709, CB-K17/1558, CB-K17/1273, CB-K17/1202, CB-K17/1196, CB-K17/1055, CB-K17/1026, CB-K17/0939, CB-K17/0917, CB-K17/0915, CB-K17/0877, CB-K17/0796, CB-K17/0724, CB-K17/0661, CB-K17/0657, CB-K17/0582, CB-K17/0581, CB-K17/0506, CB-K17/0504, CB-K17/0467, CB-K17/0345, CB-K17/0098, CB-K17/0089, CB-K17/0086, CB-K17/0082, CB-K16/1837, CB-K16/1830, CB-K16/1635, CB-K16/1630, CB-K16/1624, CB-K16/1622, CB-K16/1500, CB-K16/1465, CB-K16/1307, CB-K16/1296, DFN-CERT-2019-0068, DFN-CERT-2018-1296, DFN-CERT-2018-0323, DFN-CERT-2017-2070, DFN-CERT-2017-1954, DFN-CERT-2017-1885, DFN-CERT-2017-1831, DFN-CERT-2017-1821, DFN-CERT-2017-1785, DFN-CERT-2017-1626, DFN-CERT-2017-1326, DFN-CERT-2017-1239, DFN-CERT-2017-1238, DFN-CERT-2017-1090, DFN-CERT-2017-1060, DFN-CERT-2017-0968, DFN-CERT-2017-0947, DFN-CERT-2017-0946, DFN-CERT-2017-0904, DFN-CERT-2017-0816, DFN-CERT-2017-0746, DFN-CERT-2017-0677, DFN-CERT-2017-0675, DFN-CERT-2017-0611, DFN-CERT-2017-0609, DFN-CERT-2017-0522, DFN-CERT-2017-0519, DFN-CERT-2017-0482, DFN-CERT-2017-0351, DFN-CERT-2017-0090, DFN-CERT-2017-0089, DFN-CERT-2017-0088, DFN-CERT-2017-0086, DFN-CERT-2016-1943, DFN-CERT-2016-1937, DFN-CERT-2016-1732, DFN-CERT-2016-1726, DFN-CERT-2016-1715, DFN-CERT-2016-1714, DFN-CERT-2016-1588, DFN-CERT-2016-1555, DFN-CERT-2016-1391, DFN-CERT-2016-1378

Other: https://bettercrypto.org/
https://mozilla.github.io/server-side-tls/ssl-config-generator/
https://sweet32.info/

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

'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

'Weak' cipher suites accepted by this service via the TLSv1.2 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: 4.3) 3269/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

'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

'Weak' cipher suites accepted by this service via the TLSv1.2 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: 4.3) 636/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

'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

'Weak' cipher suites accepted by this service via the TLSv1.2 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: 4.3) 443/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

'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

'Weak' cipher suites accepted by this service via the TLSv1.2 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/

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: 623055
Packet 2: 624131

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: http://www.ietf.org/rfc/rfc1323.txt