Scan Report

February 11, 2020

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "UTC", which is abbreviated "UTC". The task was "Full and Fast - [redacted]". The scan started at Tue Feb 11 21:31:07 2020 UTC and ended at Tue Feb 11 23:38:49 2020 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
192.168.10.100	1	9	1	0	0
192.168.10.13 WSUS.[redacted]	2	3	1	0	0
192.168.10.170 Vaylin.[redacted]	4	3	0	0	0
192.168.10.1	1	5	1	0	0
192.168.10.10 AD02.[redacted]	0	2	1	0	0
192.168.10.11 AD01.[redacted]	0	2	1	0	0
192.168.10.45 infra-kali.[redacted]	0	1	0	0	0
192.168.10.128	0	0	1	0	0
192.168.10.130	0	0	1	0	0
192.168.10.132	0	0	1	0	0
192.168.10.29	0	0	1	0	0
192.168.10.30	0	0	1	0	0
192.168.10.31	0	0	1	0	0
192.168.10.61 storage.[redacted]	0	0	1	0	0
Total: 14	8	25	12	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 45 results selected by the filtering described above. Before filtering there were 574 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.10.13 - WSUS.[redacted]	SMB	Success	Protocol SMB, Port 445, User [redacted]
192.168.10.170 - Vaylin.[redacted]	SMB	Success	Protocol SMB, Port 445, User [redacted]
192.168.10.10 - AD02.[redacted]	SMB	Success	Protocol SMB, Port 445, User [redacted]

... (continues) ...

... (continued) ...

Host	Protocol	Result	Port/User
192.168.10.11 - AD01.[redacted]	SMB	Success	Protocol SMB, Port 445, User [redacted]

2 Results per Host

2.1 192.168.10.100

Host scan start Tue Feb 11 21:37:54 2020 UTC
Host scan end Tue Feb 11 23:11:23 2020 UTC

Service (Port)	Threat Level
623/tcp	High
623/udp	Medium
22/tcp	Medium
443/tcp	Medium
general/tcp	Low

2.1.1 High 623/tcp

High (CVSS: 10.0)
NVT: IPMI Cipher Zero Authentication Bypass Vulnerability

Summary
Intelligent Platform Management Interface is prone to an authentication- bypass vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Attackers can exploit this issue to gain administrative access to the device and disclose sensitive information.

Solution
Solution type: VendorFix
Ask the Vendor for an update.

Vulnerability Insight
The remote IPMI service accepted a session open request for cipher zero.

Vulnerability Detection Method
Send a request with a zero cipher and check if this request was accepted.
Details: `IPMI Cipher Zero Authentication Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103840
Version used: `$Revision: 11865 $`

... continues on next page ...

... continued from previous page ...

References
Other:
URL:http://fish2.com/ipmi/cipherzero.html

[return to 192.168.10.100]

2.1.2 Medium 623/udp

Medium (CVSS: 5.1)
NVT: IPMI MD2 Auth Type Support Enabled

Summary
IPMI MD2 auth type support is enabled on the remote host.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: Workaround
Disable MD2 auth type support.

Vulnerability Detection Method
Details: IPMI MD2 Auth Type Support Enabled
OID:1.3.6.1.4.1.25623.1.0.103839
Version used: $Revision: 11865 $

[return to 192.168.10.100]

2.1.3 Medium 22/tcp

Medium (CVSS: 4.3)
NVT: SSH Weak Encryption Algorithms Supported

Summary
The remote SSH server is configured to allow weak encryption algorithms.

Vulnerability Detection Result
The following weak client-to-server encryption algorithms are supported by the r
↪emote service:
arcfour128
arcfour256
The following weak server-to-client encryption algorithms are supported by the r
↪emote service:

... continues on next page ...

... continued from previous page ...

arcfour128
arcfour256

Solution
Solution type: Mitigation
Disable the weak encryption algorithms.

Vulnerability Insight
The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Check if remote ssh service supports Arcfour, none or CBC ciphers.
Details: SSH Weak Encryption Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: $Revision: 13581 $

References
Other:
URL:https://tools.ietf.org/html/rfc4253#section-6.3
URL:https://www.kb.cert.org/vuls/id/958563

[return to 192.168.10.100]

2.1.4 Medium 443/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Summary
The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result
The certificate of the remote service expired on 2019-09-15 22:47:28.
Certificate details:
subject ...: CN=iDRAC6 default certificate,OU=Remote Access Group,O=Dell Inc.,L=
↪Round Rock,ST=Texas,C=US
subject alternative names (SAN):
None
issued by .: CN=iDRAC6 default certificate,OU=Remote Access Group,O=Dell Inc.,L=
↪Round Rock,ST=Texas,C=US

... continues on next page ...

... continued from previous page ...

```
serial ....: 01
valid from : 2009-09-17 22:47:28 UTC
valid until: 2019-09-15 22:47:28 UTC
fingerprint (SHA-1): EADE8C43459B1FBEB106309268AF75D66D39B7FD
fingerprint (SHA-256): 03A07B1ED2A33266B8ABDE02F429C71F365E66E9C1462317C8BF8682F
↪D9BC1C3
```

Solution
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `$Revision: 11103 $`

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

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_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_DHE_RSA_WITH_DES_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_DHE_RSA_WITH_DES_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_DHE_RSA_WITH_DES_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
```

Solution
Solution type: Mitigation

... continues on next page ...

... continued from previous page ...

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

Medium (CVSS: 4.3)
NVT: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)

Summary
This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack.

Vulnerability Detection Result
```
'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
```

Impact
Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Solution
Solution type: VendorFix
- Remove support for 'DHE_EXPORT' cipher suites from the service
- If running OpenSSL updateto version 1.0.2b or 1.0.1n or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
- Hosts accepting 'DHE_EXPORT' cipher suites
- OpenSSL version before 1.0.2b and 1.0.1n

Vulnerability Insight
Flaw is triggered when handling Diffie-Hellman key exchanges defined in the 'DHE_EXPORT' cipher suites.

Vulnerability Detection Method
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)
OID:1.3.6.1.4.1.25623.1.0.805188
Version used: $Revision: 11872 $

References
CVE: CVE-2015-4000
BID:74733
Other:
URL:https://weakdh.org
URL:https://weakdh.org/imperfect-forward-secrecy.pdf
URL:http://openwall.com/lists/oss-security/2015/05/20/8
URL:https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained
URL:https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-change
↪s

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

Summary
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

Vulnerability Detection Result
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5

... continues on next page ...

... continued from previous page ...

TLS_RSA_EXPORT_WITH_RC4_40_MD5

Impact
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Solution
Solution type: VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

Affected Software/OS
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

Vulnerability Insight
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

Vulnerability Detection Method
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: 2019-07-05T09:29:25+0000

References
CVE: CVE-2015-0204
BID:71936
Other:
URL:https://freakattack.com
URL:http://secpod.org/blog/?p=3818
URL:http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-f
↪actoring-nsa.html

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

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

... continues on next page ...

... continued from previous page ...

'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_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

... continues on next page ...

... continued from previous page ...

Other:
URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-
↪1465_update_6.html
URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result
Server Temporary Key Size: 1024 bits

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: $Revision: 12865 $

References
Other:
URL:https://weakdh.org/
URL:https://weakdh.org/sysadmin.html

... continues on next page ...

... continued from previous page ...

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

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=iDRAC6 default certificate,OU=Remote Access Group,O=Del
↪l Inc.,L=Round Rock,ST=Texas,C=US
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:
  URL:https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with
```

... continues on next page ...

... continued from previous page ...

↪-sha-1-based-signature-algorithms/

[return to 192.168.10.100]

2.1.5 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: 703464618
Packet 2: 703464726

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

... continues on next page ...

... continued from previous page ...

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

[return to 192.168.10.100]

2.2 192.168.10.13

Host scan start Tue Feb 11 21:36:49 2020 UTC
Host scan end Tue Feb 11 22:56:28 2020 UTC

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

2.2.1 High general/tcp

High (CVSS: 10.0)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4534271)

Summary
This host is missing a critical security update according to Microsoft KB4534271

Vulnerability Detection Result

```
Vulnerable range:  10.0.14393.0 - 10.0.14393.3442
File checked:      C:\Windows\system32\User32.dll
File version:      10.0.14393.3383
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code, elevate privilges, disclose sensitive information, conduct denial of service and spoofing attacks.

Solution
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 10 Version 1607 x32/x64
- Microsoft Windows Server 2016

Vulnerability Insight
Multiple flaws exist due to,

... continues on next page ...

... continued from previous page ...

- Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory.
- Windows Search Indexer improperly handles objects in memory.
- win32k component improperly provides kernel information.
- Microsoft Windows Graphics Component improperly handles objects in memory.
- Microsoft Windows implements predictable memory section names.
- Windows Media Service allows file creation in arbitrary locations.
- Internet Explorer improperly accesses objects in memory.
- Windows Graphics Device Interface Plus (GDI+) improperly handles objects in memory.
- Remote Desktop Web Access improperly handles credential information.

For more information about the vulnerabilities refer Reference links.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Microsoft Windows Multiple Vulnerabilities (KB4534271)`

OID:1.3.6.1.4.1.25623.1.0.815742

Version used: `2020-01-15T14:29:04+0000`

References

```
CVE: CVE-2020-0601, CVE-2020-0607, CVE-2020-0612, CVE-2020-0615, CVE-2020-0617,
↪CVE-2020-0623, CVE-2020-0608, CVE-2020-0609, CVE-2020-0610, CVE-2020-0611, CVE
↪-2020-0614, CVE-2020-0613, CVE-2020-0620, CVE-2020-0622, CVE-2020-0625, CVE-20
↪20-0626, CVE-2020-0627, CVE-2020-0628, CVE-2020-0629, CVE-2020-0630, CVE-2020-
↪0631, CVE-2020-0632, CVE-2020-0633, CVE-2020-0634, CVE-2020-0635, CVE-2020-063
↪7, CVE-2020-0639, CVE-2020-0644, CVE-2020-0641, CVE-2020-0642, CVE-2020-0643,
↪CVE-2020-0606, CVE-2020-0646, CVE-2020-0640, CVE-2020-0605
Other:
  URL:https://support.microsoft.com/en-us/help/4534271
```

High (CVSS: 9.3)

NVT: Windows IExpress Untrusted Search Path Vulnerability

Summary

This host has IExpress bundled with Microsoft Windows and is prone to an untrusted search path vulnerability.

Vulnerability Detection Result

```
Fixed version:      Workaround
File checked:       C:\Windows\system32\IEXPRESS.EXE
File version:       11.0.14393.2007
```

Impact

Successful exploitation will allow an attacker to execute arbitrary code with the privilege of the user invoking a vulnerable self-extracting archive file.

Solution

Solution type: Workaround

... continues on next page ...

... continued from previous page ...

As a workaround save self-extracting archive files into a newly created directory, and confirm there are no unrelated files in the directory and make sure there are no suspicious files in the directory where self-extracting archive files are saved.

Affected Software/OS
IExpress bundled with Microsoft Windows

Vulnerability Insight
The flaw exists due to an untrusted search path error in self-extracting archive files created by IExpress bundled with Microsoft Windows.

Vulnerability Detection Method
Check for the presence of IExpress (IEXPRESS.EXE).
Details: `Windows IExpress Untrusted Search Path Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.813808
Version used: `$Revision: 12120 $`

References
```
CVE: CVE-2018-0598
Other:
  URL:http://jvn.jp/en/jp/JVN72748502/index.html
   URL:https://blogs.technet.microsoft.com/srd/2018/04/04/triaging-a-dll-plantin
↪g-vulnerability
```

[return to 192.168.10.13]

2.2.2 Medium 3389/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

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
```

... continues on next page ...

... continued from previous page ...

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
Other:
URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html
URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/

[return to 192.168.10.13]

2.2.3 Medium general/tcp

Medium (CVSS: 6.9)
NVT: MS Windows HID Functionality (Over USB) Code Execution Vulnerability

Summary
This host is installed with a USB device driver software and is prone to a code execution vulnerability.

Vulnerability Detection Result
File checked for existence: C:\Windows\system32\hidserv.dll

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allows user-assisted attackers to execute arbitrary programs via crafted USB data.

Solution
Solution type: Workaround
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
A workaround is to introduce device filtering on the target host to only allow trusted USB devices to be enabled automatically. Once this workaround is in place an Overwrite for this vulnerability can be created to mark it as a false positive.

Affected Software/OS
All Microsoft Windows systems with an enabled USB device driver and no local protection mechanism against the automatic enabling of additional Human Interface Device (HID).

Vulnerability Insight
The flaw is due to error in USB device driver (hidserv.dll), which does not properly warn the user before enabling additional Human Interface Device (HID) functionality.

Vulnerability Detection Method
Details: `MS Windows HID Functionality (Over USB) Code Execution Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801581
Version used: `$Revision: 11987 $`

References
`CVE: CVE-2011-0638`
`Other:`
`URL:http://www.cs.gmu.edu/~astavrou/publications.html`
`URL:http://news.cnet.com/8301-27080_3-20028919-245.html`
`URL:http://www.blackhat.com/html/bh-dc-11/bh-dc-11-briefings.html#Stavrou`

[return to 192.168.10.13]

2.2.4 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.

Vulnerability Detection Result
`Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p`

... continues on next page ...

... continued from previous page ...

```
↪rotocol:
Port: 49664/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.13[49664]
Port: 49665/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.13[49665]
     Annotation: Event log TCPIP
Port: 49668/tcp
     UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.13[49668]
     Annotation: UserMgrCli
     UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.13[49668]
     UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.13[49668]
     Annotation: Proxy Manager provider server endpoint
     UUID: 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2
     Endpoint: ncacn_ip_tcp:192.168.10.13[49668]
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.13[49668]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.13[49668]
     Annotation: IP Transition Configuration endpoint
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.13[49668]
     UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.13[49668]
     Annotation: UserMgrCli
     UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.13[49668]
     Annotation: Proxy Manager client server endpoint
     UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.13[49668]
     Annotation: Adh APIs
Port: 49669/tcp
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_ip_tcp:192.168.10.13[49669]
     Annotation: RemoteAccessCheck
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.13[49669]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.13[49669]
     Annotation: Ngc Pop Key Service
```

... continues on next page ...

... continued from previous page ...

```
      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.13[49669]
      Annotation: Ngc Pop Key Service
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:192.168.10.13[49669]
      Annotation: KeyIso
Port: 49670/tcp
      UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.13[49670]
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.13[49670]
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.13[49670]
      UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.13[49670]
      UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.13[49670]
Port: 49710/tcp
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.13[49710]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
      UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.13[49710]
      Annotation: Ngc Pop Key Service
      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.13[49710]
      Annotation: Ngc Pop Key Service
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:192.168.10.13[49710]
      Annotation: KeyIso
Port: 49711/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:192.168.10.13[49711]
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

... continues on next page ...

... continued from previous page ...

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 192.168.10.13]

2.2.5 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: 2630862496
Packet 2: 2630863615
```

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.

... continues on next page ...

... continued from previous page ...

Details: TCP timestamps
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: $Revision: 14310 $

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

[return to 192.168.10.13]

2.3 192.168.10.170

Host scan start Tue Feb 11 21:32:54 2020 UTC
Host scan end Tue Feb 11 22:57:01 2020 UTC

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

2.3.1 High general/tcp

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Updates(mfsa_2020-03_2020-03)-Windows

Product detection result
cpe:/a:mozilla:firefox:x64:71.0
Detected by Mozilla Firefox Version Detection (Windows) (OID: 1.3.6.1.4.1.25623.
↪1.0.800014)

Summary
This host is installed with Mozilla Firefox and is prone to type confusion vulnerability.

Vulnerability Detection Result
Installed version: 71.0
Fixed version: 72.0.1
Installation
path / port: C:\Program Files\Mozilla Firefox

Impact
Successful exploitation allow attackers to execute arbitrary code in the context of the user running the affected applications. Failed exploit attempts will likely cause a denial-of-service condition.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to Mozilla Firefox version 72.0.1 or later. Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 72.0.1 on Windows.

Vulnerability Insight
The flaw is due to an incorrect alias information in IonMonkey JIT compiler for setting array elements.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Mozilla Firefox Security Updates(mfsa_2020-03_2020-03)-Windows`
OID:1.3.6.1.4.1.25623.1.0.815885
Version used: `2020-01-09T13:20:19+0000`

Product Detection Result
Product: `cpe:/a:mozilla:firefox:x64:71.0`
Method: `Mozilla Firefox Version Detection (Windows)`
OID: 1.3.6.1.4.1.25623.1.0.800014)

References
`CVE: CVE-2019-17026`
`Other:`
`URL:https://www.mozilla.org/en-US/security/advisories/mfsa2020-03/`
`URL:https://www.mozilla.org/en-US/firefox/`

High (CVSS: 10.0)
NVT: Microsoft Windows Multiple Vulnerabilities (KB4534273)

Summary
This host is missing a critical security update according to Microsoft KB4534273

Vulnerability Detection Result
`Vulnerable range: 10.0.17763.0 - 10.0.17763.972`
`File checked: C:\Windows\system32\User32.dll`
`File version: 10.0.17763.914`

Impact
Successful exploitation will allow an attacker to execute arbitrary code, bypass security features, elevate privilges, disclose sensitive information, and conduct denial of service and spoofing attacks.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for x64-based Systems
Windows Server 2019

Vulnerability Insight
Multiple flaws exist due to,
- Windows Common Log File System (CLFS) driver fails to properly handle objects in memory.
- Windows Search Indexer improperly handles objects in memory.
- win32k component improperly provides kernel information.
- Microsoft Windows implements predictable memory section names.
- Windows Media Service allows file creation in arbitrary locations.
- Internet Explorer improperly accesses objects in memory.
- Windows Graphics Device Interface Plus (GDI+) improperly handles objects in memory.
For more information about the vulnerabilities refer Reference links.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft Windows Multiple Vulnerabilities (KB4534273)`
OID:1.3.6.1.4.1.25623.1.0.815741
Version used: `2020-01-16T06:11:20+0000`

References
```
CVE: CVE-2020-0601, CVE-2020-0607, CVE-2020-0612, CVE-2020-0615, CVE-2020-0617,
↪CVE-2020-0623, CVE-2020-0608, CVE-2020-0609, CVE-2020-0610, CVE-2020-0611, CVE
↪-2020-0613, CVE-2020-0614, CVE-2020-0616, CVE-2020-0620, CVE-2020-0621, CVE-20
↪20-0625, CVE-2020-0626, CVE-2020-0627, CVE-2020-0628, CVE-2020-0629, CVE-2020-
↪0630, CVE-2020-0631, CVE-2020-0632, CVE-2020-0633, CVE-2020-0634, CVE-2020-063
↪5, CVE-2020-0637, CVE-2020-0638, CVE-2020-0639, CVE-2020-0644, CVE-2020-0641,
↪CVE-2020-0642, CVE-2020-0643, CVE-2020-0640
Other:
  URL:https://support.microsoft.com/en-us/help/4534273
```


High (CVSS: 10.0)
NVT: Microsoft .NET Framework Multiple RCE Vulnerabilities (KB4535101

Summary
This host is missing an important security update according to Microsoft KB4535101

Vulnerability Detection Result
```
Vulnerable range:  4.7 - 4.7.3569
File checked:      C:\Windows\Microsoft.NET\Framework64\v4.0.30319\System.workfl
↪ow.runtime.dll
```

... continues on next page ...

... continued from previous page ...

File version: 4.7.3440.0

Impact
Successful exploitation will allow an attacker to run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system.

Solution
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft .NET Framework 3.5, 4.7.2 and 4.8 on Windows 10 version 1809 and Windows Server 2019

Vulnerability Insight
Multiple flaws exists due to,
- Microsoft .NET Framework fails to check the source markup of a file.
- Microsoft .NET Framework fails to validate input properly.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Microsoft .NET Framework Multiple RCE Vulnerabilities (KB4535101
OID:1.3.6.1.4.1.25623.1.0.815898
Version used: 2020-01-24T07:57:30+0000

References
CVE: CVE-2020-0646, CVE-2020-0605, CVE-2020-0606
Other:
URL:https://support.microsoft.com/en-us/help/4535101

High (CVSS: 9.3)
NVT: Windows IExpress Untrusted Search Path Vulnerability

Summary
This host has IExpress bundled with Microsoft Windows and is prone to an untrusted search path vulnerability.

Vulnerability Detection Result
Fixed version: Workaround
File checked: C:\Windows\system32\IEXPRESS.EXE
File version: 11.0.17763.1

Impact
Successful exploitation will allow an attacker to execute arbitrary code with the privilege of the user invoking a vulnerable self-extracting archive file.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: Workaround
As a workaround save self-extracting archive files into a newly created directory, and confirm there are no unrelated files in the directory and make sure there are no suspicious files in the directory where self-extracting archive files are saved.

Affected Software/OS
IExpress bundled with Microsoft Windows

Vulnerability Insight
The flaw exists due to an untrusted search path error in self-extracting archive files created by IExpress bundled with Microsoft Windows.

Vulnerability Detection Method
Check for the presence of IExpress (IEXPRESS.EXE).
Details: `Windows IExpress Untrusted Search Path Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.813808
Version used: `$Revision: 12120 $`

References
```
CVE: CVE-2018-0598
Other:
  URL:http://jvn.jp/en/jp/JVN72748502/index.html
   URL:https://blogs.technet.microsoft.com/srd/2018/04/04/triaging-a-dll-plantin
↪g-vulnerability
```

[return to 192.168.10.170]

2.3.2 Medium general/tcp

Medium (CVSS: 6.9)
NVT: MS Windows HID Functionality (Over USB) Code Execution Vulnerability

Summary
This host is installed with a USB device driver software and is prone to a code execution vulnerability.

Vulnerability Detection Result
`File checked for existence: C:\Windows\system32\hidserv.dll`

Impact
Successful exploitation will allows user-assisted attackers to execute arbitrary programs via crafted USB data.

Solution

... continues on next page ...

... continued from previous page ...

Solution type: Workaround
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
A workaround is to introduce device filtering on the target host to only allow trusted USB devices to be enabled automatically. Once this workaround is in place an Overwrite for this vulnerability can be created to mark it as a false positive.

Affected Software/OS
All Microsoft Windows systems with an enabled USB device driver and no local protection mechanism against the automatic enabling of additional Human Interface Device (HID).

Vulnerability Insight
The flaw is due to error in USB device driver (hidserv.dll), which does not properly warn the user before enabling additional Human Interface Device (HID) functionality.

Vulnerability Detection Method
Details: `MS Windows HID Functionality (Over USB) Code Execution Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801581
Version used: `$Revision: 11987 $`

References
`CVE: CVE-2011-0638`
`Other:`
`URL:http://www.cs.gmu.edu/~astavrou/publications.html`
`URL:http://news.cnet.com/8301-27080_3-20028919-245.html`
`URL:http://www.blackhat.com/html/bh-dc-11/bh-dc-11-briefings.html#Stavrou`

Medium (CVSS: 6.8)
NVT: Mozilla Firefox Security Updates(mfsa_2020-01_2020-02)-Windows

Product detection result
```
cpe:/a:mozilla:firefox:x64:71.0
Detected by Mozilla Firefox Version Detection (Windows) (OID: 1.3.6.1.4.1.25623.
↪1.0.800014)
```

Summary
This host is installed with Mozilla Firefox and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 71.0
Fixed version:     72
Installation
path / port:       C:\Program Files\Mozilla Firefox
```

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation allow attackers to run arbitrary code, disclose sensitive information, conduct xss attacks and bypass security restrictions.

Solution
Solution type: VendorFix
Upgrade to Mozilla Firefox version 72 or later. Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 72 on Windows.

Vulnerability Insight
Multiple flaws exists due to,
- A memory corruption error in parent process during new content process initialization on Windows.
- Bypass of namespace CSS sanitization during pasting.
- A type Confusion error in XPCVariant.cpp.
- Windows Keyboard in Private Browsing Mode may retain word suggestions.
- Python files could be inadvertently executed upon opening a download.
- Content Security Policy not applied to XSL stylesheets applied to XML documents.
- Heap address disclosure in parent process during content process initialization.
- CSS sanitization does not escape HTML tags.
- NSS may negotiate TLS 1.2 or below after a TLS 1.3 HelloRetryRequest had been sent.
- Memory safety bugs.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Mozilla Firefox Security Updates(mfsa_2020-01_2020-02)-Windows`
OID:1.3.6.1.4.1.25623.1.0.815881
Version used: `2020-01-16T07:57:40+0000`

Product Detection Result
Product: `cpe:/a:mozilla:firefox:x64:71.0`
Method: `Mozilla Firefox Version Detection (Windows)`
OID: 1.3.6.1.4.1.25623.1.0.800014)

References
```
CVE: CVE-2019-17015, CVE-2019-17016, CVE-2019-17017, CVE-2019-17018, CVE-2019-17
↪019, CVE-2019-17020, CVE-2019-17021, CVE-2019-17022, CVE-2019-17023, CVE-2019-
↪17024, CVE-2019-17025
Other:
  URL:https://www.mozilla.org/en-US/security/advisories/mfsa2020-01/
   URL:https://www.mozilla.org/en-US/firefox/
```

[return to 192.168.10.170]

2.3.3 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.

Vulnerability Detection Result
```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.170[49664]
Port: 49665/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.170[49665]
     Annotation: Event log TCPIP
Port: 49666/tcp
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.170[49666]
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.170[49666]
Port: 49667/tcp
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_ip_tcp:192.168.10.170[49667]
     Annotation: RemoteAccessCheck
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.170[49667]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.170[49667]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.170[49667]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.10.170[49667]
     Annotation: KeyIso
Port: 49668/tcp
     UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.170[49668]
Port: 49669/tcp
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
```

... continues on next page ...

... continued from previous page ...

```
      Endpoint: ncacn_ip_tcp:192.168.10.170[49669]
      Annotation: RemoteAccessCheck
      UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.170[49669]
      Annotation: Ngc Pop Key Service
      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.170[49669]
      Annotation: Ngc Pop Key Service
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:192.168.10.170[49669]
      Annotation: KeyIso
Port: 49670/tcp
      UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.170[49670]
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.170[49670]
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.170[49670]
      UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.170[49670]
      UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.170[49670]
Port: 49769/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:192.168.10.170[49769]
Port: 5040/tcp
      UUID: 1a927394-352e-4553-ae3f-7cf4aafca620, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.170[5040]
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 192.168.10.170]

2.4 192.168.10.1

Host scan start Tue Feb 11 21:34:00 2020 UTC
Host scan end Tue Feb 11 22:55:53 2020 UTC

Service (Port)	Threat Level
22/tcp	High
443/tcp	Medium
80/tcp	Medium
22/tcp	Medium
22/tcp	Low

2.4.1 High 22/tcp

High (CVSS: 7.5)
NVT: Deprecated SSH-1 Protocol Detection

Summary
The host is running SSH and is providing / accepting one or more deprecated versions of the SSH protocol which have known cryptograhic flaws.

Vulnerability Detection Result
```
The service is providing / accepting the following deprecated versions of the SS
↪H protocol which have known cryptograhic flaws:
1.5
```

Impact
Successful exploitation could allows remote attackers to bypass security restrictions and to obtain a client's public host key during a connection attempt and use it to open and authenticate an SSH session to another server with the same access.

Solution
Solution type: VendorFix
Reconfigure the SSH service to only provide / accept the SSH protocol version SSH-2.

Affected Software/OS
Services providing / accepting the SSH protocol version SSH-1 (1.33 and 1.5).

Vulnerability Detection Method
Details: `Deprecated SSH-1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.801993
Version used: `$Revision: 13586 $`

References
`CVE: CVE-2001-0361, CVE-2001-0572, CVE-2001-1473`
`BID:2344`
`Other:`

. . . continues on next page . . .

... continued from previous page ...

URL:http://www.kb.cert.org/vuls/id/684820
URL:http://xforce.iss.net/xforce/xfdb/6603

[return to 192.168.10.1]

2.4.2 Medium 443/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

Summary
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Vulnerability Detection Result
The service is only providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.802067) NVT.

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Solution
Solution type: Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

Vulnerability Insight
The SSLv2 and SSLv3 protocols containing known cryptographic flaws like:
- Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566)
- Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)

Vulnerability Detection Method
Check the used protocols of the services provided by this system.
Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: $Revision: 5547 $

References
CVE: CVE-2016-0800, CVE-2014-3566
Other:

... continues on next page ...

... continued from previous page ...

URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report
URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
URL:https://drownattack.com/
URL:https://www.imperialviolet.org/2014/10/14/poodle.html

Medium (CVSS: 4.3)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

Summary
This host is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

Solution
Solution type: Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

Vulnerability Insight
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method
Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ...
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: $Revision: 11402 $

References
CVE: CVE-2014-3566
BID:70574
Other:
URL:https://www.openssl.org/~bodo/ssl-poodle.pdf
URL:https://www.imperialviolet.org/2014/10/14/poodle.html
URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit

... continues on next page ...

... continued from previous page ...

↪ing-ssl-30.html

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

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 SSLv3 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
Other:
URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-
↪1465_update_6.html
URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/

[return to 192.168.10.1]

2.4.3 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result
```
The following URLs requires Basic Authentication (URL:realm name):
http://192.168.10.1/:"level_15_access"
http://192.168.10.1/archive:"level_15_access"
http://192.168.10.1/banner:"level_15_access"
http://192.168.10.1/exec:"level_15_access"
http://192.168.10.1/help:"level_15_access"
http://192.168.10.1/template:"level_15_access"
```

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `$Revision: 10726 $`

References
```
Other:
  URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_S
↪ession_Management
   URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
```

... continues on next page ...

... continued from previous page ...

URL:https://cwe.mitre.org/data/definitions/319.html

[return to 192.168.10.1]

2.4.4 Medium 22/tcp

Medium (CVSS: 4.3)
NVT: SSH Weak Encryption Algorithms Supported

Summary
The remote SSH server is configured to allow weak encryption algorithms.

Vulnerability Detection Result

```
The following weak client-to-server encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
The following weak server-to-client encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
```

Solution
Solution type: Mitigation
Disable the weak encryption algorithms.

Vulnerability Insight
The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Check if remote ssh service supports Arcfour, none or CBC ciphers.
Details: SSH Weak Encryption Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: $Revision: 13581 $

References

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:https://tools.ietf.org/html/rfc4253#section-6.3
   URL:https://www.kb.cert.org/vuls/id/958563
```

[return to 192.168.10.1]

2.4.5 Low 22/tcp

Low (CVSS: 2.6)
NVT: SSH Weak MAC Algorithms Supported

Summary
The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

Vulnerability Detection Result

```
The following weak client-to-server MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
```

Solution
Solution type: Mitigation
Disable the weak MAC algorithms.

Vulnerability Detection Method
Details: `SSH Weak MAC Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `$Revision: 13581 $`

[return to 192.168.10.1]

2.5 192.168.10.10

Host scan start Tue Feb 11 22:13:57 2020 UTC
Host scan end Tue Feb 11 23:07:42 2020 UTC

Service (Port)	Threat Level
3389/tcp	Medium
135/tcp	Medium

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
general/tcp	Low

2.5.1 Medium 3389/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

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

... continues on next page ...

... continued from previous page ...

```
CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:
  URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-
↪1465_update_6.html
   URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
```

[return to 192.168.10.10]

2.5.2 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.

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.10[49664]
Port: 49665/tcp
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.10[49665]
     Annotation: DHCP Client LRPC Endpoint
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.10[49665]
     Annotation: Event log TCPIP
Port: 49666/tcp
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_ip_tcp:192.168.10.10[49666]
     Annotation: RemoteAccessCheck
     UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
     Endpoint: ncacn_ip_tcp:192.168.10.10[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:192.168.10.10[49666]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : LSA access
```

... continues on next page ...

... continued from previous page ...

```
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[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:192.168.10.10[49666]
      Annotation: Ngc Pop Key Service
      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49666]
      Annotation: Ngc Pop Key Service
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:192.168.10.10[49666]
      Annotation: KeyIso
      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49666]
      Annotation: Impl friendly name
      UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
      Endpoint: ncacn_ip_tcp:192.168.10.10[49666]
      Annotation: MS NT Directory DRS Interface
Port: 49668/tcp
      UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
      Annotation: UserMgrCli
      UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
      Annotation: AppInfo
      UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
      UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
      Annotation: Proxy Manager provider server endpoint
      UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
      UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
      UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
      Annotation: IP Transition Configuration endpoint
      UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
      Annotation: AppInfo
      UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
      Annotation: AppInfo
      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
```

... continues on next page ...

... continued from previous page ...

```
      UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
      Annotation: UserMgrCli
      UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
      Annotation: Proxy Manager client server endpoint
      UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
      Annotation: Adh APIs
      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
      Annotation: Impl friendly name
      UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
      UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
      Annotation: AppInfo
      UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49668]
      Annotation: AppInfo
Port: 49669/tcp
      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
      Endpoint: ncacn_ip_tcp:192.168.10.10[49669]
      Annotation: RemoteAccessCheck
      UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49669]
      Named pipe : lsass
      Win32 service or process : Netlogon
      Description : Net Logon service
      UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
      Endpoint: ncacn_ip_tcp:192.168.10.10[49669]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : LSA access
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49669]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
      UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49669]
      Annotation: Ngc Pop Key Service
      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49669]
      Annotation: Ngc Pop Key Service
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:192.168.10.10[49669]
```

... continues on next page ...

... continued from previous page ...

```
      Annotation: KeyIso
      UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
      Endpoint: ncacn_ip_tcp:192.168.10.10[49669]
      Annotation: MS NT Directory DRS Interface
Port: 49670/tcp
      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
      Endpoint: ncacn_http:192.168.10.10[49670]
      Annotation: RemoteAccessCheck
      UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
      Endpoint: ncacn_http:192.168.10.10[49670]
      Named pipe : lsass
      Win32 service or process : Netlogon
      Description : Net Logon service
      UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
      Endpoint: ncacn_http:192.168.10.10[49670]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : LSA access
      UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
      Endpoint: ncacn_http:192.168.10.10[49670]
      Annotation: Ngc Pop Key Service
      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
      Endpoint: ncacn_http:192.168.10.10[49670]
      Annotation: Ngc Pop Key Service
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_http:192.168.10.10[49670]
      Annotation: KeyIso
      UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
      Endpoint: ncacn_http:192.168.10.10[49670]
      Annotation: MS NT Directory DRS Interface
Port: 49671/tcp
      UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49671]
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49671]
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49671]
      UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49671]
      UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49671]
Port: 49730/tcp
      UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[49730]
```

... continues on next page ...

... continued from previous page ...

```
      Annotation: Frs2 Service
Port: 64770/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:192.168.10.10[64770]
Port: 64781/tcp
      UUID: 5b821720-f63b-11d0-aad2-00c04fc324db, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[64781]
      UUID: 6bffd098-a112-3610-9833-46c3f874532d, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.10[64781]
Port: 64800/tcp
      UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5
      Endpoint: ncacn_ip_tcp:192.168.10.10[64800]
      Named pipe : dnsserver
      Win32 service or process : dns.exe
      Description : DNS Server
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 192.168.10.10]

2.5.3 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: 1290797618
Packet 2: 1290798742
```

... continues on next page ...

... continued from previous page ...

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

[return to 192.168.10.10]

2.6 192.168.10.11

Host scan start Tue Feb 11 21:42:54 2020 UTC
Host scan end Tue Feb 11 22:45:02 2020 UTC

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

2.6.1 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.

Vulnerability Detection Result
```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
      UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49664]
Port: 49665/tcp
      UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49665]
      Annotation: Event log TCPIP
Port: 49667/tcp
      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
      Endpoint: ncacn_ip_tcp:192.168.10.11[49667]
      Annotation: RemoteAccessCheck
      UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49667]
      Named pipe : lsass
      Win32 service or process : Netlogon
      Description : Net Logon service
      UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
      Endpoint: ncacn_ip_tcp:192.168.10.11[49667]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : LSA access
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49667]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
      UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49667]
      Annotation: Ngc Pop Key Service
      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49667]
      Annotation: Ngc Pop Key Service
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:192.168.10.11[49667]
      Annotation: KeyIso
```

... continues on next page ...

... continued from previous page ...

```
      UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
      Endpoint: ncacn_ip_tcp:192.168.10.11[49667]
      Annotation: MS NT Directory DRS Interface
Port: 49668/tcp
      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
      Endpoint: ncacn_ip_tcp:192.168.10.11[49668]
      Annotation: RemoteAccessCheck
      UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49668]
      Named pipe : lsass
      Win32 service or process : Netlogon
      Description : Net Logon service
      UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
      Endpoint: ncacn_ip_tcp:192.168.10.11[49668]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : LSA access
      UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49668]
      Annotation: Ngc Pop Key Service
      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49668]
      Annotation: Ngc Pop Key Service
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:192.168.10.11[49668]
      Annotation: KeyIso
      UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
      Endpoint: ncacn_ip_tcp:192.168.10.11[49668]
      Annotation: MS NT Directory DRS Interface
Port: 49669/tcp
      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
      Endpoint: ncacn_http:192.168.10.11[49669]
      Annotation: RemoteAccessCheck
      UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
      Endpoint: ncacn_http:192.168.10.11[49669]
      Named pipe : lsass
      Win32 service or process : Netlogon
      Description : Net Logon service
      UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
      Endpoint: ncacn_http:192.168.10.11[49669]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : LSA access
      UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
      Endpoint: ncacn_http:192.168.10.11[49669]
      Annotation: Ngc Pop Key Service
      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
```

... continues on next page ...

... continued from previous page ...

```
      Endpoint: ncacn_http:192.168.10.11[49669]
      Annotation: Ngc Pop Key Service
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_http:192.168.10.11[49669]
      Annotation: KeyIso
      UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
      Endpoint: ncacn_http:192.168.10.11[49669]
      Annotation: MS NT Directory DRS Interface
Port: 49672/tcp
      UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      Annotation: UserMgrCli
      UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      Named pipe : atsvc
      Win32 service or process : mstask.exe
      Description : Scheduler service
      UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      Annotation: AppInfo
      UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      Annotation: Proxy Manager provider server endpoint
      UUID: 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      Annotation: IP Transition Configuration endpoint
      UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      Annotation: AppInfo
      UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      Annotation: AppInfo
      UUID: 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      Annotation: Vpn APIs
      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
```

... continues on next page ...

... continued from previous page ...

```
      Annotation: UserMgrCli
      UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      Annotation: Proxy Manager client server endpoint
      UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      Annotation: Adh APIs
      UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      UUID: fb9a3757-cff0-4db0-b9fc-bd6c131612fd, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      Annotation: AppInfo
      UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49672]
      Annotation: AppInfo
Port: 49675/tcp
      UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49675]
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[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:192.168.10.11[49675]
      UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49675]
      UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[49675]
Port: 60571/tcp
      UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5
      Endpoint: ncacn_ip_tcp:192.168.10.11[60571]
      Named pipe : dnsserver
      Win32 service or process : dns.exe
      Description : DNS Server
Port: 64523/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:192.168.10.11[64523]
Port: 64532/tcp
      UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.11[64532]
      Annotation: Frs2 Service
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

... continues on next page ...

... continued from previous page ...

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 192.168.10.11]

2.6.2 Medium 3389/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

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).

... continues on next page ...

... continued from previous page ...

- 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
Other:
URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html
URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/

[return to 192.168.10.11]

2.6.3 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: 3188123673
Packet 2: 3188124769

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.

... continues on next page ...

... continued from previous page ...

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

[return to 192.168.10.11]

2.7 192.168.10.45

Host scan start	Tue Feb 11 21:35:05 2020 UTC
Host scan end	Tue Feb 11 22:12:33 2020 UTC

Service (Port)	Threat Level
8000/tcp	Medium

2.7.1 Medium 8000/tcp

Medium (CVSS: 5.0)
NVT: Missing 'httpOnly' Cookie Attribute

Summary
The application is missing the 'httpOnly' cookie attribute

Vulnerability Detection Result
```
The cookies:
Set-Cookie:  csrftoken=xjQGkXqwpp8z2G4xN6A92MFBuEtIcicGlWv1yPJgZ72vGmVDetYMkSJzO
↪uPQ9QXo; expires=Tue, 09 Feb 2021 21:35:07 GMT; Max-Age=***replaced***; Path=/
↪; SameSite=Lax
are missing the "httpOnly" attribute.
```

Solution

... continues on next page ...

... continued from previous page ...

Solution type: Mitigation
Set the 'httpOnly' attribute for any session cookie.

Affected Software/OS
Application with session handling in cookies.

Vulnerability Insight
The flaw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Vulnerability Detection Method
Check all cookies sent by the application for a missing 'httpOnly' attribute
Details: `Missing 'httpOnly' Cookie Attribute`
OID:1.3.6.1.4.1.25623.1.0.105925
Version used: `2019-11-21T13:29:18+0000`

References
```
Other:
  URL:https://www.owasp.org/index.php/HttpOnly
   URL:https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-
↪002)
```

[return to 192.168.10.45]

2.8 192.168.10.128

Host scan start	Tue Feb 11 21:33:11 2020 UTC
Host scan end	Tue Feb 11 22:46:35 2020 UTC

Service (Port)	Threat Level
general/tcp	Low

2.8.1 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: 2591530678
Packet 2: 2293732017
```

... continues on next page ...

... continued from previous page ...

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

[return to 192.168.10.128]

2.9 192.168.10.130

Host scan start Tue Feb 11 21:32:02 2020 UTC
Host scan end Tue Feb 11 22:36:18 2020 UTC

Service (Port)	Threat Level
general/tcp	Low

2.9.1 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: 4101218427
Packet 2: 3618779876
```

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

[return to 192.168.10.130]

2.10 192.168.10.132

Host scan start	Tue Feb 11 21:35:19 2020 UTC
Host scan end	Tue Feb 11 22:38:53 2020 UTC

Service (Port)	Threat Level
general/tcp	Low

2.10.1 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: 4070539813
Packet 2: 4070540957
```

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

. . . continues on next page . . .

... continued from previous page ...

Version used: $Revision: 14310 $

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

[return to 192.168.10.132]

2.11 192.168.10.29

Host scan start Tue Feb 11 21:34:33 2020 UTC
Host scan end Tue Feb 11 23:27:50 2020 UTC

Service (Port)	Threat Level
general/tcp	Low

2.11.1 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: 1434709775
Packet 2: 1434709884

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.

... continues on next page ...

. . . continued from previous page . . .

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

[return to 192.168.10.29]

2.12 192.168.10.30

Host scan start	Tue Feb 11 21:39:52 2020 UTC
Host scan end	Tue Feb 11 23:30:20 2020 UTC

Service (Port)	Threat Level
general/tcp	Low

2.12.1 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: 1434594839
Packet 2: 1434594946
```

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

. . . continues on next page . . .

... continued from previous page ...

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

[return to 192.168.10.30]

2.13 192.168.10.31

Host scan start	Tue Feb 11 21:32:19 2020 UTC
Host scan end	Tue Feb 11 23:27:04 2020 UTC

Service (Port)	Threat Level
general/tcp	Low

2.13.1 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary

... continues on next page ...

... continued from previous page ...

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: 1434445987
Packet 2: 1434446095

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

[return to 192.168.10.31]

2.14 192.168.10.61

Host scan start	Tue Feb 11 21:32:37 2020 UTC
Host scan end	Tue Feb 11 22:35:02 2020 UTC

Service (Port)	Threat Level
general/tcp	Low

2.14.1 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: 2765154531
Packet 2: 3922411009
```

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

... continues on next page ...

... continued from previous page ...

URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152

[return to 192.168.10.61]

This file was automatically generated.