1Windows XP VM scan

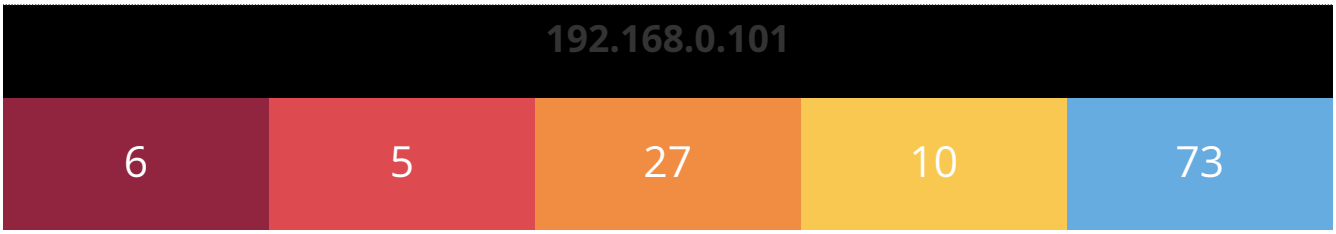
Report generated by Nessus™ Sat, 27 Aug 2022 15:00:56 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.0.101 4

Vulnerabilities by Host



Scan Information

Start time: Sat Aug 27 14:38:13 2022
End time: Sat Aug 27 15:00:55 2022

Host Information

Netbios Name: HHHTESTSERVER
IP: 192.168.0.101
MAC Address: 58:FB:84:D7:C7:D3 00:0C:29:BB:80:80
OS: Microsoft Windows XP, Microsoft Windows XP for Embedded Systems

Vulnerabilities

125313 - Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)

Synopsis

The remote host is affected by a remote code execution vulnerability.

Description

The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.

See Also

http://www.nessus.org/u?577af692

http://www.nessus.org/u?8e4e0b74

Solution

Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.7 (CVSS2#E:H/RL:OF/RC:C)

References

BID	108273
CVE	CVE-2019-0708
XREF	CISA-KNOWN-EXPLOITED:2022/05/03

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2019/05/22, Modified: 2022/08/15

Plugin Output

tcp/3389

73182 - Microsoft Windows XP Unsupported Installation Detection

Synopsis

The remote operating system is no longer supported.

Description

The remote host is running Microsoft Windows XP. Support for this operating system by Microsoft ended April 8th, 2014.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.

See Also

http://www.nessus.org/u?2f80aef2

http://www.nessus.org/u?321523eb

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

http://www.nessus.org/u?8dcab5e4

Solution

Upgrade to a version of Windows that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

9.0 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

XREF	EDB-ID:41929
XREF	IAVA:0001-A-0023

Plugin Information

Published: 2014/03/25, Modified: 2020/09/22

Plugin Output

tcp/0

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

Plugin Output

tcp/443

```
- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Low Strength Ciphers (<= 64-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    EXP-EDH-RSA-DES-CBC-SHA                         DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA                             DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA                             DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5                                 DH(512)       None     RC4(40)                 MD5
       export
    ADH-DES-CBC-SHA                                 DH            None     DES-CBC(56)
 SHA1
    EXP1024-DES-CBC-SHA                             RSA(1024)     RSA      DES-CBC(56)
 SHA1      export
    EXP1024-RC2-CBC-MD5                             RSA(1024)     RSA      RC2-CBC(56)             MD5
       export
    EXP1024-RC4-MD5                                 RSA(1024)     RSA      RC4(56)                 MD5
       export
    EXP1024-RC4-SHA                                 RSA(1024)     RSA      RC4(56)
 SHA1      export
    DES-CBC-SHA                                     RSA           RSA      DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    EDH-RSA-DES-CBC3-SHA                            DH            RSA      3DES-CBC(168)
 SHA1
    ADH-DES-CBC3-SHA                                DH            None     3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                                    RSA           RSA      3DES-CBC(168)       [...]
```

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

Plugin Output

tcp/5003

```
- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Low Strength Ciphers (<= 64-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    EXP-EDH-RSA-DES-CBC-SHA                         DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA                             DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA                             DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5                                 DH(512)       None     RC4(40)                 MD5
       export
    ADH-DES-CBC-SHA                                 DH            None     DES-CBC(56)
 SHA1
    EXP1024-DES-CBC-SHA                             RSA(1024)     RSA      DES-CBC(56)
 SHA1      export
    EXP1024-RC2-CBC-MD5                             RSA(1024)     RSA      RC2-CBC(56)             MD5
       export
    EXP1024-RC4-MD5                                 RSA(1024)     RSA      RC4(56)                 MD5
       export
    EXP1024-RC4-SHA                                 RSA(1024)     RSA      RC4(56)
 SHA1      export
    DES-CBC-SHA                                     RSA           RSA      DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    EDH-RSA-DES-CBC3-SHA                            DH            RSA      3DES-CBC(168)
 SHA1
    ADH-DES-CBC3-SHA                                DH            None     3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                                    RSA           RSA      3DES-CBC(168)       [...]
```

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

Plugin Output

tcp/54345/loadrunner_agent

```
- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Low Strength Ciphers (<= 64-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    EXP-EDH-RSA-DES-CBC-SHA                         DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA                             DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA                             DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5                                 DH(512)       None     RC4(40)                 MD5
       export
    ADH-DES-CBC-SHA                                 DH            None     DES-CBC(56)
 SHA1
    EXP1024-DES-CBC-SHA                             RSA(1024)     RSA      DES-CBC(56)
 SHA1      export
    EXP1024-RC2-CBC-MD5                             RSA(1024)     RSA      RC2-CBC(56)             MD5
       export
    EXP1024-RC4-MD5                                 RSA(1024)     RSA      RC4(56)                 MD5
       export
    EXP1024-RC4-SHA                                 RSA(1024)     RSA      RC4(56)
 SHA1      export
    DES-CBC-SHA                                     RSA           RSA      DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    EDH-RSA-DES-CBC3-SHA                            DH            RSA      3DES-CBC(168)
 SHA1
    ADH-DES-CBC3-SHA                                DH            None     3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                                    RSA           RSA      3DES-CBC(168)       [...]
```

108797 - Unsupported Windows OS (remote)

Synopsis

The remote OS or service pack is no longer supported.

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

See Also

https://support.microsoft.com/en-us/lifecycle

Solution

Upgrade to a supported service pack or operating system

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

XREF	IAVA:0001-A-0501

Plugin Information

Published: 2018/04/03, Modified: 2022/07/05

Plugin Output

tcp/0

```
The following Windows version is installed and not supported:

Microsoft Windows XP
```

```
Microsoft Windows XP for Embedded Systems
```

58435 - MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)

Synopsis

The remote Windows host could allow arbitrary code execution.

Description

An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted.

If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.

This plugin also checks for a denial of service vulnerability in Microsoft Terminal Server.

Note that this script does not detect the vulnerability if the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting is enabled or the security layer is set to 'SSL (TLS 1.0)' on the remote host.

See Also

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2012/ms12-020

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Note that an extended support contract with Microsoft is required to obtain the patch for this vulnerability for Windows 2000.

Risk Factor

High

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

BID	52353
BID	52354
CVE	CVE-2012-0002
CVE	CVE-2012-0152
MSKB	2621440
MSKB	2667402
XREF	EDB-ID:18606
XREF	MSFT:MS12-020
XREF	IAVA:2012-A-0039

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2012/03/22, Modified: 2022/08/15

Plugin Output

tcp/3389

97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

See Also

http://www.nessus.org/u?68fc8eff

http://www.nessus.org/u?321523eb

http://www.nessus.org/u?065561d0

http://www.nessus.org/u?d9f569cf

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

http://www.nessus.org/u?b9d9ebf9

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

https://github.com/stamparm/EternalRocks/

http://www.nessus.org/u?59db5b5b

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions.

SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

High

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:H/RL:O/RC:C)

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.1 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

BID	96703
BID	96704
BID	96705
BID	96706
BID	96707
BID	96709
CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146
CVE	CVE-2017-0147
CVE	CVE-2017-0148
MSKB	4012212
MSKB	4012213
MSKB	4012214
MSKB	4012215

MSKB	4012216
MSKB	4012217
MSKB	4012606
MSKB	4013198
MSKB	4013429
MSKB	4012598
XREF	EDB-ID:41891
XREF	EDB-ID:41987
XREF	MSFT:MS17-010
XREF	IAVA:2017-A-0065
XREF	CISA-KNOWN-EXPLOITED:2022/05/03
XREF	CISA-KNOWN-EXPLOITED:2022/08/10
XREF	CISA-KNOWN-EXPLOITED:2022/04/15
XREF	CISA-KNOWN-EXPLOITED:2022/04/27
XREF	CISA-KNOWN-EXPLOITED:2022/06/14

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2017/03/20, Modified: 2022/05/25

Plugin Output

tcp/445/cifs

```
Sent:
00000054ff534d4225000000001803c800000000000000000000000021075140318000110000000
00ffffffff0000000000000000000000540000005400020023000000110000 5c00500049005000
45005c0000000000

Received:
ff534d4225050200c09803c8000000000000000000000000210751403180001000000
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/443

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ADH-DES-CBC3-SHA              0x00, 0x1B       DH            None     3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/5003

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ADH-DES-CBC3-SHA              0x00, 0x1B       DH            None     3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/54345/loadrunner_agent

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ADH-DES-CBC3-SHA              0x00, 0x1B       DH            None     3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

18405 - Remote Desktop Protocol Server Man-in-the-Middle Weakness

Synopsis

It may be possible to get access to the remote host.

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a publicly known hard-coded RSA private key. Any attacker in a privileged network location can use the key for this attack.

See Also

http://www.nessus.org/u?8033da0d

Solution

- Force the use of SSL as a transport layer for this service if supported, or/and

- On Microsoft Windows operating systems, select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

3.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	13818
CVE	CVE-2005-1794

Plugin Information

Published: 2005/06/01, Modified: 2022/08/24

Plugin Output

tcp/3389

57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

http://www.nessus.org/u?df39b8b3

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information

Published: 2012/01/19, Modified: 2021/03/15

Plugin Output

tcp/445/cifs

31705 - SSL Anonymous Cipher Suites Supported

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?3a040ada

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

Risk Factor

Low

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	28482
CVE	CVE-2007-1858

Plugin Information

Published: 2008/03/28, Modified: 2021/02/03

Plugin Output

tcp/443

```
The following is a list of SSL anonymous ciphers supported by the remote TCP server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EXP-ADH-DES-CBC-SHA           0x00, 0x19        DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5               0x00, 0x17        DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA               0x00, 0x1A        DH            None     DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    ADH-DES-CBC3-SHA              0x00, 0x1B        DH            None     3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    ADH-RC4-MD5                   0x00, 0x18        DH            None     RC4(128)               MD5

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

31705 - SSL Anonymous Cipher Suites Supported

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?3a040ada

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

Risk Factor

Low

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	28482
CVE	CVE-2007-1858

Plugin Information

Published: 2008/03/28, Modified: 2021/02/03

Plugin Output

tcp/5003

```
The following is a list of SSL anonymous ciphers supported by the remote TCP server :

  Low Strength Ciphers (<= 64-bit key)

    Name                         Code              KEX           Auth     Encryption             MAC
    -----------------------      ----------        ---           ----     ---------------------  ---
    EXP-ADH-DES-CBC-SHA          0x00, 0x19        DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5              0x00, 0x17        DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA              0x00, 0x1A        DH            None     DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                         Code              KEX           Auth     Encryption             MAC
    -----------------------      ----------        ---           ----     ---------------------  ---
    ADH-DES-CBC3-SHA             0x00, 0x1B        DH            None     3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                         Code              KEX           Auth     Encryption             MAC
    -----------------------      ----------        ---           ----     ---------------------  ---
    ADH-RC4-MD5                  0x00, 0x18        DH            None     RC4(128)               MD5

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

31705 - SSL Anonymous Cipher Suites Supported

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?3a040ada

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

Risk Factor

Low

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	28482
CVE	CVE-2007-1858

Plugin Information

Published: 2008/03/28, Modified: 2021/02/03

Plugin Output

tcp/54345/loadrunner_agent

```
The following is a list of SSL anonymous ciphers supported by the remote TCP server :

  Low Strength Ciphers (<= 64-bit key)

    Name                        Code              KEX           Auth     Encryption             MAC
    ----------------------      ----------        ---           ----     ---------------------  ---
    EXP-ADH-DES-CBC-SHA         0x00, 0x19        DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5             0x00, 0x17        DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA             0x00, 0x1A        DH            None     DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                        Code              KEX           Auth     Encryption             MAC
    ----------------------      ----------        ---           ----     ---------------------  ---
    ADH-DES-CBC3-SHA            0x00, 0x1B        DH            None     3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                        Code              KEX           Auth     Encryption             MAC
    ----------------------      ----------        ---           ----     ---------------------  ---
    ADH-RC4-MD5                 0x00, 0x18        DH            None     RC4(128)               MD5

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/443

```
The following certificates were part of the certificate chain
sent by the remote host, but they have expired :

|-Subject   : C=IL/O=Mercury Interactive/CN=Mercury Interactive e-Cert CA
|-Not After : Jun 23 00:00:00 2015 GMT

|-Subject   : C=IL/O=Mercury Interactive/OU=/E=/CN=test
|-Not After : Jun 23 00:00:00 2015 GMT

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=IL/O=Mercury Interactive/CN=Mercury Interactive e-Cert CA
|-Issuer  : C=IL/O=Mercury Interactive/CN=Mercury Interactive e-Cert CA
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/5003

```
The following certificates were part of the certificate chain
sent by the remote host, but they have expired :

|-Subject   : C=IL/O=Mercury Interactive/CN=Mercury Interactive e-Cert CA
|-Not After : Jun 23 00:00:00 2015 GMT

|-Subject   : C=IL/O=Mercury Interactive/OU=/E=/CN=test
|-Not After : Jun 23 00:00:00 2015 GMT

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=IL/O=Mercury Interactive/CN=Mercury Interactive e-Cert CA
|-Issuer  : C=IL/O=Mercury Interactive/CN=Mercury Interactive e-Cert CA
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/54345/loadrunner_agent

```
The following certificates were part of the certificate chain
sent by the remote host, but they have expired :

|-Subject   : C=IL/O=Mercury Interactive/CN=Mercury Interactive e-Cert CA
|-Not After : Jun 23 00:00:00 2015 GMT

|-Subject   : C=IL/O=Mercury Interactive/OU=/E=/CN=test
|-Not After : Jun 23 00:00:00 2015 GMT

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=IL/O=Mercury Interactive/CN=Mercury Interactive e-Cert CA
|-Issuer  : C=IL/O=Mercury Interactive/CN=Mercury Interactive e-Cert CA
```

15901 - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution

Purchase or generate a new SSL certificate to replace the existing one.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2004/12/03, Modified: 2021/02/03

Plugin Output

tcp/443

```
The SSL certificate has already expired :

  Subject          : C=IL, O=Mercury Interactive, OU=, emailAddress=, CN=test
  Issuer           : C=IL, O=Mercury Interactive, CN=Mercury Interactive e-Cert CA
  Not valid before : Jun 22 23:00:00 2005 GMT
  Not valid after  : Jun 23 00:00:00 2015 GMT
```

15901 - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution

Purchase or generate a new SSL certificate to replace the existing one.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2004/12/03, Modified: 2021/02/03

Plugin Output

tcp/5003

```
The SSL certificate has already expired :

  Subject          : C=IL, O=Mercury Interactive, OU=, emailAddress=, CN=test
  Issuer           : C=IL, O=Mercury Interactive, CN=Mercury Interactive e-Cert CA
  Not valid before : Jun 22 23:00:00 2005 GMT
  Not valid after  : Jun 23 00:00:00 2015 GMT
```

15901 - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution

Purchase or generate a new SSL certificate to replace the existing one.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2004/12/03, Modified: 2021/02/03

Plugin Output

tcp/54345/loadrunner_agent

```
The SSL certificate has already expired :

  Subject          : C=IL, O=Mercury Interactive, OU=, emailAddress=, CN=test
  Issuer           : C=IL, O=Mercury Interactive, CN=Mercury Interactive e-Cert CA
  Not valid before : Jun 22 23:00:00 2005 GMT
  Not valid after  : Jun 23 00:00:00 2015 GMT
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/443

```
The identities known by Nessus are :

  192.168.0.101
  192.168.0.101

The Common Name in the certificate is :

  test
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/5003

```
The identities known by Nessus are :

  192.168.0.101
  192.168.0.101

The Common Name in the certificate is :

  test
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/54345/loadrunner_agent

```
The identities known by Nessus are :

  192.168.0.101
  192.168.0.101

The Common Name in the certificate is :

  test
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/

http://www.nessus.org/u?ac7327a0

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:ND/RC:C)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/443

```
List of RC4 cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EXP-ADH-RC4-MD5               0x00, 0x17        DH(512)       None     RC4(40)                MD5
       export
    EXP1024-RC4-MD5               0x00, 0x60        RSA(1024)     RSA      RC4(56)                MD5
       export
    EXP1024-RC4-SHA               0x00, 0x64        RSA(1024)     RSA      RC4(56)
 SHA1      export

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    ADH-RC4-MD5                   0x00, 0x18        DH            None     RC4(128)               MD5
    RC4-MD5                       0x00, 0x04        RSA           RSA      RC4(128)               MD5
    RC4-SHA                       0x00, 0x05        RSA           RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/

http://www.nessus.org/u?ac7327a0

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:ND/RC:C)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/5003

```
List of RC4 cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     --------------------   ---
    EXP-ADH-RC4-MD5               0x00, 0x17        DH(512)       None     RC4(40)                MD5
       export
    EXP1024-RC4-MD5               0x00, 0x60        RSA(1024)     RSA      RC4(56)                MD5
       export
    EXP1024-RC4-SHA               0x00, 0x64        RSA(1024)     RSA      RC4(56)
 SHA1      export

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     --------------------   ---
    ADH-RC4-MD5                   0x00, 0x18        DH            None     RC4(128)               MD5
    RC4-MD5                       0x00, 0x04        RSA           RSA      RC4(128)               MD5
    RC4-SHA                       0x00, 0x05        RSA           RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/

http://www.nessus.org/u?ac7327a0

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:ND/RC:C)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/54345/loadrunner_agent

```
List of RC4 cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     --------------------   ---
    EXP-ADH-RC4-MD5               0x00, 0x17        DH(512)       None     RC4(40)                MD5
       export
    EXP1024-RC4-MD5               0x00, 0x60        RSA(1024)     RSA      RC4(56)                MD5
       export
    EXP1024-RC4-SHA               0x00, 0x64        RSA(1024)     RSA      RC4(56)
 SHA1      export

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     --------------------   ---
    ADH-RC4-MD5                   0x00, 0x18        DH            None     RC4(128)               MD5
    RC4-MD5                       0x00, 0x04        RSA           RSA      RC4(128)               MD5
    RC4-SHA                       0x00, 0x05        RSA           RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/443

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=IL/O=Mercury Interactive/CN=Mercury Interactive e-Cert CA
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/5003

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=IL/O=Mercury Interactive/CN=Mercury Interactive e-Cert CA
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/54345/loadrunner_agent

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=IL/O=Mercury Interactive/CN=Mercury Interactive e-Cert CA
```

26928 - SSL Weak Cipher Suites Supported

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer weak encryption.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?6527892d

Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

XREF	CWE:326
XREF	CWE:327
XREF	CWE:720
XREF	CWE:753
XREF	CWE:803
XREF	CWE:928
XREF	CWE:934

Plugin Information

Published: 2007/10/08, Modified: 2021/02/03

Plugin Output

tcp/443

```
Here is the list of weak SSL ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15       DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA           0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5               0x00, 0x17       DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA               0x00, 0x1A       DH            None     DES-CBC(56)
 SHA1
    EXP1024-DES-CBC-SHA           0x00, 0x62       RSA(1024)     RSA      DES-CBC(56)
 SHA1      export
    EXP1024-RC2-CBC-MD5           0x00, 0x61       RSA(1024)     RSA      RC2-CBC(56)            MD5
       export
    EXP1024-RC4-MD5               0x00, 0x60       RSA(1024)     RSA      RC4(56)                MD5
       export
    EXP1024-RC4-SHA               0x00, 0x64       RSA(1024)     RSA      RC4(56)
 SHA1      export
    DES-CBC-SHA                   0x00, 0x09       RSA           RSA      DES-CBC(56)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

26928 - SSL Weak Cipher Suites Supported

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer weak encryption.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?6527892d

Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

XREF	CWE:326
XREF	CWE:327
XREF	CWE:720
XREF	CWE:753
XREF	CWE:803
XREF	CWE:928
XREF	CWE:934

Plugin Information

Published: 2007/10/08, Modified: 2021/02/03

Plugin Output

tcp/5003

```
Here is the list of weak SSL ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                         Code             KEX           Auth     Encryption             MAC
    ---------------------        ----------       ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA      0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA          0x00, 0x15       DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA          0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5              0x00, 0x17       DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA              0x00, 0x1A       DH            None     DES-CBC(56)
 SHA1
    EXP1024-DES-CBC-SHA          0x00, 0x62       RSA(1024)     RSA      DES-CBC(56)
 SHA1      export
    EXP1024-RC2-CBC-MD5          0x00, 0x61       RSA(1024)     RSA      RC2-CBC(56)            MD5
       export
    EXP1024-RC4-MD5              0x00, 0x60       RSA(1024)     RSA      RC4(56)                MD5
       export
    EXP1024-RC4-SHA              0x00, 0x64       RSA(1024)     RSA      RC4(56)
 SHA1      export
    DES-CBC-SHA                  0x00, 0x09       RSA           RSA      DES-CBC(56)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

26928 - SSL Weak Cipher Suites Supported

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer weak encryption.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?6527892d

Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

XREF	CWE:326
XREF	CWE:327
XREF	CWE:720
XREF	CWE:753
XREF	CWE:803
XREF	CWE:928
XREF	CWE:934

Plugin Information

Published: 2007/10/08, Modified: 2021/02/03

Plugin Output

tcp/54345/loadrunner_agent

```
Here is the list of weak SSL ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                         Code              KEX           Auth     Encryption             MAC
    ---------------------        ----------        ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA      0x00, 0x14        DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA          0x00, 0x15        DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA          0x00, 0x19        DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5              0x00, 0x17        DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA              0x00, 0x1A        DH            None     DES-CBC(56)
 SHA1
    EXP1024-DES-CBC-SHA          0x00, 0x62        RSA(1024)     RSA      DES-CBC(56)
 SHA1      export
    EXP1024-RC2-CBC-MD5          0x00, 0x61        RSA(1024)     RSA      RC2-CBC(56)            MD5
       export
    EXP1024-RC4-MD5              0x00, 0x60        RSA(1024)     RSA      RC4(56)                MD5
       export
    EXP1024-RC4-SHA              0x00, 0x64        RSA(1024)     RSA      RC4(56)
 SHA1      export
    DES-CBC-SHA                  0x00, 0x09        RSA           RSA      DES-CBC(56)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS v3.0 Base Score

6.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	70574
CVE	CVE-2014-3566
XREF	CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2020/06/12

Plugin Output

tcp/443

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is not supported on the server. Mitigating this
vulnerability requires SSLv3 to be disabled and TLSv1 or newer to be enabled.
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS v3.0 Base Score

6.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	70574
CVE	CVE-2014-3566
XREF	CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2020/06/12

Plugin Output

tcp/5003

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is not supported on the server. Mitigating this
vulnerability requires SSLv3 to be disabled and TLSv1 or newer to be enabled.
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS v3.0 Base Score

6.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	70574
CVE	CVE-2014-3566
XREF	CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2020/06/12

Plugin Output

tcp/54345/loadrunner_agent

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is not supported on the server. Mitigating this
vulnerability requires SSLv3 to be disabled and TLSv1 or newer to be enabled.
```

57690 - Terminal Services Encryption Level is Medium or Low

Synopsis

The remote host is using weak cryptography.

Description

The remote Terminal Services service is not configured to use strong cryptography.

Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.

Solution

Change RDP encryption level to one of :

3. High

4. FIPS Compliant

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2012/01/25, Modified: 2022/08/15

Plugin Output

tcp/3389

```
The terminal services encryption level is set to :

2. Medium
```

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis

The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Description

At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.

Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

See Also

https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Solution

Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Risk Factor

Low

Plugin Information

Published: 2013/09/03, Modified: 2018/11/15

Plugin Output

tcp/443

```
The following certificates were part of the certificate chain
sent by the remote host, but contain RSA keys that are considered
to be weak :

|-Subject        : C=IL/O=Mercury Interactive/OU=/E=/CN=test
|-RSA Key Length : 1024 bits
```

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis

The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Description

At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.

Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

See Also

https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Solution

Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Risk Factor

Low

Plugin Information

Published: 2013/09/03, Modified: 2018/11/15

Plugin Output

tcp/5003

```
The following certificates were part of the certificate chain
sent by the remote host, but contain RSA keys that are considered
to be weak :

|-Subject        : C=IL/O=Mercury Interactive/OU=/E=/CN=test
|-RSA Key Length : 1024 bits
```

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis

The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Description

At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.

Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

See Also

https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Solution

Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Risk Factor

Low

Plugin Information

Published: 2013/09/03, Modified: 2018/11/15

Plugin Output

tcp/54345/loadrunner_agent

```
The following certificates were part of the certificate chain
sent by the remote host, but contain RSA keys that are considered
to be weak :

|-Subject        : C=IL/O=Mercury Interactive/OU=/E=/CN=test
|-RSA Key Length : 1024 bits
```

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

See Also

https://weakdh.org/

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

3.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	74733
CVE	CVE-2015-4000

Plugin Information

Published: 2015/05/28, Modified: 2022/06/28

Plugin Output

tcp/443

```
Vulnerable connection combinations :

  SSL/TLS version  : SSLv3
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_DES_CBC_SHA
  Diffie-Hellman MODP size (bits) : 512
  Logjam attack difficulty : Easy (could be carried out by individuals)

  SSL/TLS version  : SSLv3
  Cipher suite     : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
  Diffie-Hellman MODP size (bits) : 512
  Logjam attack difficulty : Easy (could be carried out by individuals)

  SSL/TLS version  : SSLv3
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_3DES_EDE_CBC_SHA
  Diffie-Hellman MODP size (bits) : 512
  Logjam attack difficulty : Easy (could be carried out by individuals)
```

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

See Also

https://weakdh.org/

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

3.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	74733
CVE	CVE-2015-4000

Plugin Information

Published: 2015/05/28, Modified: 2022/06/28

Plugin Output

tcp/5003

```
Vulnerable connection combinations :

  SSL/TLS version  : SSLv3
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_DES_CBC_SHA
  Diffie-Hellman MODP size (bits) : 512
  Logjam attack difficulty : Easy (could be carried out by individuals)

  SSL/TLS version  : SSLv3
  Cipher suite     : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
  Diffie-Hellman MODP size (bits) : 512
  Logjam attack difficulty : Easy (could be carried out by individuals)

  SSL/TLS version  : SSLv3
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_3DES_EDE_CBC_SHA
  Diffie-Hellman MODP size (bits) : 512
  Logjam attack difficulty : Easy (could be carried out by individuals)
```

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

See Also

https://weakdh.org/

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

3.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	74733
CVE	CVE-2015-4000

Plugin Information

Published: 2015/05/28, Modified: 2022/06/28

Plugin Output

tcp/54345/loadrunner_agent

```
Vulnerable connection combinations :

  SSL/TLS version  : SSLv3
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_DES_CBC_SHA
  Diffie-Hellman MODP size (bits) : 512
  Logjam attack difficulty : Easy (could be carried out by individuals)

  SSL/TLS version  : SSLv3
  Cipher suite     : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
  Diffie-Hellman MODP size (bits) : 512
  Logjam attack difficulty : Easy (could be carried out by individuals)

  SSL/TLS version  : SSLv3
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_3DES_EDE_CBC_SHA
  Diffie-Hellman MODP size (bits) : 512
  Logjam attack difficulty : Easy (could be carried out by individuals)
```

83738 - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.

See Also

https://weakdh.org/

Solution

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

3.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

2.2 (CVSS2#E:U/RL:ND/RC:C)

References

BID	74733
CVE	CVE-2015-4000

Plugin Information

Published: 2015/05/21, Modified: 2021/02/03

Plugin Output

tcp/443

```
EXPORT_DHE cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                         Code             KEX           Auth     Encryption             MAC
    ----------------------       ----------       ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA      0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EXP-ADH-DES-CBC-SHA          0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5              0x00, 0x17       DH(512)       None     RC4(40)                MD5
       export

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

83738 - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.

See Also

https://weakdh.org/

Solution

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

3.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

2.2 (CVSS2#E:U/RL:ND/RC:C)

References

BID	74733
CVE	CVE-2015-4000

Plugin Information

Published: 2015/05/21, Modified: 2021/02/03

Plugin Output

tcp/5003

```
EXPORT_DHE cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                         Code              KEX           Auth     Encryption             MAC
    ----------------------       ----------        ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA      0x00, 0x14        DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EXP-ADH-DES-CBC-SHA          0x00, 0x19        DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5              0x00, 0x17        DH(512)       None     RC4(40)                MD5
       export

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

83738 - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.

See Also

https://weakdh.org/

Solution

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

3.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

2.2 (CVSS2#E:U/RL:ND/RC:C)

References

BID	74733
CVE	CVE-2015-4000

Plugin Information

Published: 2015/05/21, Modified: 2021/02/03

Plugin Output

tcp/54345/loadrunner_agent

```
EXPORT_DHE cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                         Code             KEX           Auth     Encryption             MAC
    ----------------------       ----------       ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA      0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EXP-ADH-DES-CBC-SHA          0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5              0x00, 0x17       DH(512)       None     RC4(40)                MD5
       export

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

30218 - Terminal Services Encryption Level is not FIPS-140 Compliant

Synopsis

The remote host is not FIPS-140 compliant.

Description

The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.

Solution

Change RDP encryption level to :

4. FIPS Compliant

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2008/02/11, Modified: 2022/08/15

Plugin Output

tcp/3389

```
The terminal services encryption level is set to :

2. Medium (Client Compatible)
```

39446 - Apache Tomcat Detection

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

See Also

https://tomcat.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0535

Plugin Information

Published: 2009/06/18, Modified: 2020/09/22

Plugin Output

tcp/8080/www

```
URL     : http://192.168.0.101:8080/
Version : unknown
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2022/08/22

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_xp -> Microsoft Windows XP

Following application CPE matched on the remote system :

  cpe:/a:apache:tomcat -> Apache Software Foundation Tomcat
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 99
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

58:FB:84:D7:C7:D3 : Intel Corporate
00:0C:29:BB:80:80 : VMware, Inc.
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 58:FB:84:D7:C7:D3
  - 00:0C:29:BB:80:80
```

24326 - HP LoadRunner Agent Service Detection

Synopsis

An HP LoadRunner Agent is listening on the remote host.

Description

An HP LoadRunner Agent is listening on the remote host. This agent enables a LoadRunner Controller to communicate with the LoadRunner Load Generator on the remote host for performance testing. Note that Hewlett-Packard acquired LoadRunner in November 2006 as part of its acquisition of Mercury Interactive.

See Also

http://www.nessus.org/u?90911f10

http://www.nessus.org/u?7ea6b97b

Solution

Limit incoming traffic to this port to hosts using the LoadRunner Controller.

Risk Factor

None

Plugin Information

Published: 2007/02/13, Modified: 2022/06/01

Plugin Output

tcp/54345/loadrunner_agent

```
HP LoadRunner was found to be listening and has a secure channel enabled.
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/8080/www

```
Based on the response to an OPTIONS request :

  - HTTP methods  DELETE  HEAD  OPTIONS  POST  PUT  TRACE GET
    are allowed on :

    /
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/2869/www

```
The remote web server type is :

Microsoft-HTTPAPI/1.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/8080/www

```
The remote web server type is :

Apache-Coyote/1.1
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2869/www

```
Response Code : HTTP/1.1 400 Bad Request

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html
  Server: Microsoft-HTTPAPI/1.0
  Date: Sat, 27 Aug 2022 09:16:10 GMT
  Connection: close
  Content-Length: 39

Response Body :

<h1>Bad Request (Invalid Hostname)</h1>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/8080/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
Headers :

  ETag: W/"177-1389346906625"
  Last-Modified: Fri, 10 Jan 2014 09:41:46 GMT
  Content-Type: text/html
  Content-Length: 177
  Date: Sat, 27 Aug 2022 09:16:10 GMT
  Server: Apache-Coyote/1.1
  Connection: close

Response Body :

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
  <META HTTP-EQUIV="Refresh" CONTENT="1;URL=/crm/HomePage.do">
</head>
<body>
<br>
</body>
```

```
</html>
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

CVSS v3.0 Base Score

0.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

CVSS v2.0 Base Score

0.0 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:N)

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2019/10/04

Plugin Output

icmp/0

```
The ICMP timestamps seem to be in little endian format (not in network format)
The difference between the local and remote clocks is -1 seconds.
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Windows 5.1
The remote native LAN manager is : Windows 2000 LAN Manager
The remote SMB Domain Name is : HHHTESTSERVER
```

26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.

If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access'

service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0506

Plugin Information

Published: 2007/10/04, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
Could not connect to the registry because:
Could not connect to \winreg
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/139/smb

```
An SMB server is running on this port.
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/445/cifs

```
A CIFS server is running on this port.
```

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :
  SMBv1
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

Plugin Output

tcp/445/cifs

```
The remote host does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.0        Windows 8
3.0.2      Windows 8.1
3.1        Windows 10
3.1.1      Windows 10
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/08/15

Plugin Output

tcp/135/epmap

```
Port 135/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/08/15

Plugin Output

tcp/139/smb

```
Port 139/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/08/15

Plugin Output

tcp/443

```
Port 443/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/08/15

Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/08/15

Plugin Output

tcp/2869/www

```
Port 2869/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/08/15

Plugin Output

tcp/3389

```
Port 3389/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/08/15

Plugin Output

tcp/5001

```
Port 5001/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/08/15

Plugin Output

tcp/5002

```
Port 5002/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/08/15

Plugin Output

tcp/5003

```
Port 5003/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/08/15

Plugin Output

tcp/8080/www

```
Port 8080/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/08/15

Plugin Output

tcp/54345/loadrunner_agent

```
Port 54345/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2022/06/09

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.3.0
Nessus build : 20080
Plugin feed version : 202208270351
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : 1Windows XP VM scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.0.107
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 1552.687 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Scan Start Date : 2022/8/27 14:38 India Standard Time
Scan duration : 1345 sec
```

24786 - Nessus Windows Scan Not Performed with Admin Privileges

Synopsis

The Nessus scan of this host may be incomplete due to insufficient privileges provided.

Description

The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.

Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.

If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

References

XREF IAVB:0001-B-0505

Plugin Information

Published: 2007/03/12, Modified: 2020/09/22

Plugin Output

tcp/0

```
It was not possible to connect to '\\HHHTESTSERVER\ADMIN$' with the supplied credentials.
```

10884 - Network Time Protocol (NTP) Server Detection

Synopsis

An NTP server is listening on the remote host.

Description

An NTP server is listening on port 123. If not securely configured, it may provide information about its version, current date, current time, and possibly system information.

See Also

http://www.ntp.org

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0934

Plugin Information

Published: 2015/03/20, Modified: 2021/02/24

Plugin Output

udp/123/ntp

```
An NTP service has been discovered, listening on port 123.

No sensitive information has been disclosed.

Version : unknown
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2022/03/09

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows XP
Microsoft Windows XP for Embedded Systems
Confidence level : 99
Method : MSRPC

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

RDP:000000000f00000010000100080001000900000001001000100010
NTP:!:unknown
HTTP:Server: Microsoft-HTTPAPI/1.0

SinFP:
   P1:B11113:F0x12:W64240:O0204ffff:M1460:
   P2:B11113:F0x12:W64240:O0204ffff010303000101080a0000000000000000001010402:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:190300_7_p=443
SSLcert:!:i/CN:Mercury Interactive e-Cert CAi/O:Mercury Interactives/CN:tests/O:Mercury Interactive
82b086f69358c34feb139f3197f5408100cc26c6
i/CN:Mercury Interactive e-Cert CAi/O:Mercury Interactives/CN:tests/O:Mercury Interactive
82b086f69358c34feb139f3197f5408100cc26c6



The remote host is running one of these operating systems :
```

```
Microsoft Windows XP
Microsoft Windows XP for Embedded Systems
```

117886 - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
    Message     :
Credentials were not provided for detected SMB service.
```

10919 - Open Port Re-check

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.

There are several possible reasons for this :

- The scan may have caused a service to freeze or stop running.

- An administrator may have stopped a particular service during the scanning process.

This might be an availability problem related to the following :

- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.

- This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.

- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again.

Solution

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF IAVB:0001-B-0509

Plugin Information

Published: 2002/03/19, Modified: 2021/07/23

Plugin Output

tcp/0

```
Port 5001 was detected as being open but is now closed
```

```
Port 5003 was detected as being open but is now closed
Port 5002 was detected as being open but is now closed
Port 54345 was detected as being open but is now closed
Port 443 was detected as being open but is now closed
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2022/08/15

Plugin Output

tcp/0

```
. You need to take the following action :

[ Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check) (125313) ]

+ Action to take : Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008
 R2.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

66173 - RDP Screenshot

Synopsis

It is possible to take a screenshot of the remote login screen.

Description

This script attempts to connect to the remote host via RDP (Remote Desktop Protocol) and attempts to take a screenshot of the login screen.

While this is not a vulnerability by itself, some versions of Windows display the names of the users who can connect and which ones are connected already.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/04/22, Modified: 2022/08/15

Plugin Output

tcp/3389

```
It was possible to gather the following screenshot of the remote login screen.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/443

```
This port supports SSLv3.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/5003

```
This port supports SSLv3.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/54345/loadrunner_agent

```
This port supports SSLv3.
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/443

```
The host name known by Nessus is :

  hhhtestserver

The Common Name in the certificate is :

  test
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/5003

```
The host name known by Nessus is :

  hhhtestserver

The Common Name in the certificate is :

  test
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/54345/loadrunner_agent

```
The host name known by Nessus is :

  hhhtestserver

The Common Name in the certificate is :

  test
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/443

```
Subject Name:

Country: IL
Organization: Mercury Interactive
Organization Unit:
Email Address:
Common Name: test

Issuer Name:

Country: IL
Organization: Mercury Interactive
Common Name: Mercury Interactive e-Cert CA

Serial Number: 64

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jun 22 23:00:00 2005 GMT
Not Valid After: Jun 23 00:00:00 2015 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D7 61 78 6A AB 09 D9 C8 3F 6D F4 19 F0 E6 41 21 5B AC 7F
            AA 4C 93 7C E9 72 EE 5A 4F 60 52 A3 00 EB 4B 08 BE D1 0E 53
            08 C3 E0 95 E2 39 9B 83 1E 59 19 53 8D 6A 81 5D 88 B3 E0 46
            AF 02 C5 93 BA 8B BF B2 27 06 24 5E ED B3 F1 E5 B6 5E E2 AB
            77 21 5E E5 47 06 89 0E 71 53 D6 87 8F 63 14 F8 49 7F FC 0E
```

```
            E1 1A 91 92 F9 57 41 5E 82 72 44 AB DB 57 94 B8 66 7D AA 41
            42 8F D9 F1 7D 0B 6B 8E 99
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 05 0C 58 E9 BF 2A 99 65 6B 21 6B B5 A0 4D 50 3C 83 C3 C3
           89 3C CD 56 A1 86 E8 19 E2 54 32 2E 2D 29 5C F6 27 B1 05 7D
           22 3B E8 18 D0 53 62 E5 E5 6B 1E 08 C4 1B 28 B5 52 64 0E 86
           C7 0B 32 6A 6D 7E BE 06 D8 2D A2 66 EF 6C 2A 55 C2 1B BA 6F
           93 DE 00 A3 60 18 EC 68 8E D1 7D 43 92 88 45 4E 46 1F 47 CA
           05 AB DD 02 57 82 2D 93 22 3C 36 91 88 8A E3 1B 74 2E 4F 5E
           DD B5 E5 D8 BC F9 61 3B 77 49 AD E2 6C 3A 1F FE A9 AC BD C4
           B0 27 EA BD 67 E1 A1 B3 1D 74 A9 9A 29 1A 94 B2 C3 8D 59 10
           42 A6 B2 8E F2 9F 58 AD 52 76 14 33 1E 50 C6 85 BE 1D B2 2D
           E0 57 88 4F 4B 92 73 22 9A 5C 2B 57 78 45 2D A1 49 08 BE CB
           FC 3D 89 84 9E 5F 82 D4 AE 94 AC 38 42 B1 56 98 D2 F4 F0 59
           FB 7E 7B C2 A1 62 30 58 A6 90 14 73 7D C4 59 88 9C 7A 76 AD
           AE 70 B7 48 28 FD 7E 89 9A C6 3A 81 4F 24 97 0C E6

Fingerprints :

SHA-256 Fingerprint: C1 17 B1 1A 2B A6 60 F7 2A 68 29 58 67 3B DE A3 0B 04 D0 E6
                     4A 47 3 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/5003

```
Subject Name:

Country: IL
Organization: Mercury Interactive
Organization Unit:
Email Address:
Common Name: test

Issuer Name:

Country: IL
Organization: Mercury Interactive
Common Name: Mercury Interactive e-Cert CA

Serial Number: 64

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jun 22 23:00:00 2005 GMT
Not Valid After: Jun 23 00:00:00 2015 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D7 61 78 6A AB 09 D9 C8 3F 6D F4 19 F0 E6 41 21 5B AC 7F
            AA 4C 93 7C E9 72 EE 5A 4F 60 52 A3 00 EB 4B 08 BE D1 0E 53
            08 C3 E0 95 E2 39 9B 83 1E 59 19 53 8D 6A 81 5D 88 B3 E0 46
            AF 02 C5 93 BA 8B BF B2 27 06 24 5E ED B3 F1 E5 B6 5E E2 AB
            77 21 5E E5 47 06 89 0E 71 53 D6 87 8F 63 14 F8 49 7F FC 0E
```

```
            E1 1A 91 92 F9 57 41 5E 82 72 44 AB DB 57 94 B8 66 7D AA 41
            42 8F D9 F1 7D 0B 6B 8E 99
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 05 0C 58 E9 BF 2A 99 65 6B 21 6B B5 A0 4D 50 3C 83 C3 C3
           89 3C CD 56 A1 86 E8 19 E2 54 32 2E 2D 29 5C F6 27 B1 05 7D
           22 3B E8 18 D0 53 62 E5 E5 6B 1E 08 C4 1B 28 B5 52 64 0E 86
           C7 0B 32 6A 6D 7E BE 06 D8 2D A2 66 EF 6C 2A 55 C2 1B BA 6F
           93 DE 00 A3 60 18 EC 68 8E D1 7D 43 92 88 45 4E 46 1F 47 CA
           05 AB DD 02 57 82 2D 93 22 3C 36 91 88 8A E3 1B 74 2E 4F 5E
           DD B5 E5 D8 BC F9 61 3B 77 49 AD E2 6C 3A 1F FE A9 AC BD C4
           B0 27 EA BD 67 E1 A1 B3 1D 74 A9 9A 29 1A 94 B2 C3 8D 59 10
           42 A6 B2 8E F2 9F 58 AD 52 76 14 33 1E 50 C6 85 BE 1D B2 2D
           E0 57 88 4F 4B 92 73 22 9A 5C 2B 57 78 45 2D A1 49 08 BE CB
           FC 3D 89 84 9E 5F 82 D4 AE 94 AC 38 42 B1 56 98 D2 F4 F0 59
           FB 7E 7B C2 A1 62 30 58 A6 90 14 73 7D C4 59 88 9C 7A 76 AD
           AE 70 B7 48 28 FD 7E 89 9A C6 3A 81 4F 24 97 0C E6

Fingerprints :

SHA-256 Fingerprint: C1 17 B1 1A 2B A6 60 F7 2A 68 29 58 67 3B DE A3 0B 04 D0 E6
                     4A 47 3 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/54345/loadrunner_agent

```
Subject Name:

Country: IL
Organization: Mercury Interactive
Organization Unit:
Email Address:
Common Name: test

Issuer Name:

Country: IL
Organization: Mercury Interactive
Common Name: Mercury Interactive e-Cert CA

Serial Number: 64

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jun 22 23:00:00 2005 GMT
Not Valid After: Jun 23 00:00:00 2015 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D7 61 78 6A AB 09 D9 C8 3F 6D F4 19 F0 E6 41 21 5B AC 7F
            AA 4C 93 7C E9 72 EE 5A 4F 60 52 A3 00 EB 4B 08 BE D1 0E 53
            08 C3 E0 95 E2 39 9B 83 1E 59 19 53 8D 6A 81 5D 88 B3 E0 46
            AF 02 C5 93 BA 8B BF B2 27 06 24 5E ED B3 F1 E5 B6 5E E2 AB
            77 21 5E E5 47 06 89 0E 71 53 D6 87 8F 63 14 F8 49 7F FC 0E
```

```
            E1 1A 91 92 F9 57 41 5E 82 72 44 AB DB 57 94 B8 66 7D AA 41
            42 8F D9 F1 7D 0B 6B 8E 99
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 05 0C 58 E9 BF 2A 99 65 6B 21 6B B5 A0 4D 50 3C 83 C3 C3
           89 3C CD 56 A1 86 E8 19 E2 54 32 2E 2D 29 5C F6 27 B1 05 7D
           22 3B E8 18 D0 53 62 E5 E5 6B 1E 08 C4 1B 28 B5 52 64 0E 86
           C7 0B 32 6A 6D 7E BE 06 D8 2D A2 66 EF 6C 2A 55 C2 1B BA 6F
           93 DE 00 A3 60 18 EC 68 8E D1 7D 43 92 88 45 4E 46 1F 47 CA
           05 AB DD 02 57 82 2D 93 22 3C 36 91 88 8A E3 1B 74 2E 4F 5E
           DD B5 E5 D8 BC F9 61 3B 77 49 AD E2 6C 3A 1F FE A9 AC BD C4
           B0 27 EA BD 67 E1 A1 B3 1D 74 A9 9A 29 1A 94 B2 C3 8D 59 10
           42 A6 B2 8E F2 9F 58 AD 52 76 14 33 1E 50 C6 85 BE 1D B2 2D
           E0 57 88 4F 4B 92 73 22 9A 5C 2B 57 78 45 2D A1 49 08 BE CB
           FC 3D 89 84 9E 5F 82 D4 AE 94 AC 38 42 B1 56 98 D2 F4 F0 59
           FB 7E 7B C2 A1 62 30 58 A6 90 14 73 7D C4 59 88 9C 7A 76 AD
           AE 70 B7 48 28 FD 7E 89 9A C6 3A 81 4F 24 97 0C E6

Fingerprints :

SHA-256 Fingerprint: C1 17 B1 1A 2B A6 60 F7 2A 68 29 58 67 3B DE A3 0B 04 D0 E6
                     4A 47 3 [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/443

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14        DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15        DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA           0x00, 0x19        DH(512)       None     DES-CBC(40)
 SHA1      export
    ADH-DES-CBC-SHA               0x00, 0x1A        DH            None     DES-CBC(56)
 SHA1
    EXP1024-DES-CBC-SHA           0x00, 0x62        RSA(1024)     RSA      DES-CBC(56)
 SHA1      export
```

```
    EXP1024-RC2-CBC-MD5           0x00, 0x61       RSA(1024)     RSA      RC2-CBC(56)             MD5
       export
    DES-CBC-SHA                   0x00, 0x09       RSA           RSA      DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption              MAC
    ----------------------        ----------       ---           ----     --------------------    ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ADH-DES-CBC3-SHA              0x00, 0x1B       DH            None     3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption              MAC
    ----------------------        ----------       ---           ----     --------------------    ---
    IDEA-CBC-SHA                  0x00, 0x07       RSA           RSA      IDEA-CBC(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Ci [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/5003

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15       DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA           0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    ADH-DES-CBC-SHA               0x00, 0x1A       DH            None     DES-CBC(56)
 SHA1
    EXP1024-DES-CBC-SHA           0x00, 0x62       RSA(1024)     RSA      DES-CBC(56)
 SHA1      export
```

```
    EXP1024-RC2-CBC-MD5           0x00, 0x61       RSA(1024)     RSA      RC2-CBC(56)             MD5
       export
    DES-CBC-SHA                   0x00, 0x09       RSA           RSA      DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption              MAC
    ----------------------        ----------       ---           ----     --------------------    ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ADH-DES-CBC3-SHA              0x00, 0x1B       DH            None     3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption              MAC
    ----------------------        ----------       ---           ----     --------------------    ---
    IDEA-CBC-SHA                  0x00, 0x07       RSA           RSA      IDEA-CBC(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Ci [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/54345/loadrunner_agent

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14        DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15        DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA           0x00, 0x19        DH(512)       None     DES-CBC(40)
 SHA1      export
    ADH-DES-CBC-SHA               0x00, 0x1A        DH            None     DES-CBC(56)
 SHA1
    EXP1024-DES-CBC-SHA           0x00, 0x62        RSA(1024)     RSA      DES-CBC(56)
 SHA1      export
```

```
    EXP1024-RC2-CBC-MD5           0x00, 0x61       RSA(1024)     RSA      RC2-CBC(56)             MD5
       export
    DES-CBC-SHA                   0x00, 0x09       RSA           RSA      DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption              MAC
    ----------------------        ----------       ---           ----     --------------------    ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ADH-DES-CBC3-SHA              0x00, 0x1B       DH            None     3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption              MAC
    ----------------------        ----------       ---           ----     --------------------    ---
    IDEA-CBC-SHA                  0x00, 0x07       RSA           RSA      IDEA-CBC(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Ci [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2022/07/25

Plugin Output

tcp/443

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : SSLv3
  Low Strength Ciphers (<= 64-bit key)

    Name                        Code              KEX           Auth     Encryption             MAC
    ----------------------      ----------        ---           ----     --------------------   ---
    EXP-EDH-RSA-DES-CBC-SHA     0x00, 0x14        DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA         0x00, 0x15        DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA         0x00, 0x19        DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5             0x00, 0x17        DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA             0x00, 0x1A        DH            None     DES-CBC(56)
 SHA1
    EXP1024-DES-CBC-SHA         0x00, 0x62        RSA(1024)     RSA      DES-CBC(56)
 SHA1      export
    EXP1024-RC2-CBC-MD5         0x00, 0x61        RSA(1024)     RSA      RC2-CBC(56)            MD5
       export
```

```
   EXP1024-RC4-MD5              0x00, 0x60       RSA(1024)     RSA      RC4(56)                MD5
      export
   EXP1024-RC4-SHA              0x00, 0x64       RSA(1024)     RSA      RC4(56)
SHA1      export
   DES-CBC-SHA                  0x00, 0x09       RSA           RSA      DES-CBC(56)
SHA1

 Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

   Name                         Code             KEX           Auth     Encryption             MAC
   ----------------------       ----------       ---           ----     ---------------------  ---
   EDH-RSA-DES-CBC3-SHA         0x00, 0x16       DH            RSA      3DES-CBC(168)
SHA1
   ADH-DES-CBC3-SHA             0x00, 0x1B       DH            None     3DES-CBC(168)
SHA1
   DES-CBC3-SHA                 0x00, 0x0A       RSA           RSA      3DES-CBC(168)
SHA1

 [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2022/07/25

Plugin Output

tcp/5003

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : SSLv3
  Low Strength Ciphers (<= 64-bit key)

    Name                        Code              KEX           Auth     Encryption             MAC
    ----------------------      ----------        ---           ----     --------------------   ---
    EXP-EDH-RSA-DES-CBC-SHA     0x00, 0x14        DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA         0x00, 0x15        DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA         0x00, 0x19        DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5             0x00, 0x17        DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA             0x00, 0x1A        DH            None     DES-CBC(56)
 SHA1
    EXP1024-DES-CBC-SHA         0x00, 0x62        RSA(1024)     RSA      DES-CBC(56)
 SHA1      export
    EXP1024-RC2-CBC-MD5         0x00, 0x61        RSA(1024)     RSA      RC2-CBC(56)            MD5
       export
```

```
   EXP1024-RC4-MD5              0x00, 0x60       RSA(1024)     RSA      RC4(56)                MD5
      export
   EXP1024-RC4-SHA              0x00, 0x64       RSA(1024)     RSA      RC4(56)
SHA1      export
   DES-CBC-SHA                  0x00, 0x09       RSA           RSA      DES-CBC(56)
SHA1

 Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

   Name                         Code             KEX           Auth     Encryption             MAC
   ----------------------       ----------       ---           ----     ---------------------  ---
   EDH-RSA-DES-CBC3-SHA         0x00, 0x16       DH            RSA      3DES-CBC(168)
SHA1
   ADH-DES-CBC3-SHA             0x00, 0x1B       DH            None     3DES-CBC(168)
SHA1
   DES-CBC3-SHA                 0x00, 0x0A       RSA           RSA      3DES-CBC(168)
SHA1

 [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2022/07/25

Plugin Output

tcp/54345/loadrunner_agent

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : SSLv3
  Low Strength Ciphers (<= 64-bit key)

    Name                        Code              KEX           Auth     Encryption             MAC
    ----------------------      ----------        ---           ----     --------------------   ---
    EXP-EDH-RSA-DES-CBC-SHA     0x00, 0x14        DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA         0x00, 0x15        DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA         0x00, 0x19        DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5             0x00, 0x17        DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA             0x00, 0x1A        DH            None     DES-CBC(56)
 SHA1
    EXP1024-DES-CBC-SHA         0x00, 0x62        RSA(1024)     RSA      DES-CBC(56)
 SHA1      export
    EXP1024-RC2-CBC-MD5         0x00, 0x61        RSA(1024)     RSA      RC2-CBC(56)            MD5
       export
```

```
   EXP1024-RC4-MD5              0x00, 0x60       RSA(1024)     RSA      RC4(56)                MD5
      export
   EXP1024-RC4-SHA              0x00, 0x64       RSA(1024)     RSA      RC4(56)
SHA1      export
   DES-CBC-SHA                  0x00, 0x09       RSA           RSA      DES-CBC(56)
SHA1

 Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

   Name                         Code             KEX           Auth     Encryption             MAC
   ----------------------       ----------       ---           ----     ---------------------  ---
   EDH-RSA-DES-CBC3-SHA         0x00, 0x16       DH            RSA      3DES-CBC(168)
SHA1
   ADH-DES-CBC3-SHA             0x00, 0x1B       DH            None     3DES-CBC(168)
SHA1
   DES-CBC3-SHA                 0x00, 0x0A       RSA           RSA      3DES-CBC(168)
SHA1

 [...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/443

```
Here is the list of SSL PFS ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14        DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15        DH            RSA      DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
 SHA1
```

```
The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/5003

```
Here is the list of SSL PFS ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14        DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15        DH            RSA      DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
 SHA1
```

```
The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/54345/loadrunner_agent

```
Here is the list of SSL PFS ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14        DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15        DH            RSA      DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
 SHA1
```

```
The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

Plugin Output

tcp/443

```
This port supports resuming SSLv3 sessions.
```

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

Plugin Output

tcp/5003

```
This port supports resuming SSLv3 sessions.
```

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

Plugin Output

tcp/54345/loadrunner_agent

```
This port supports resuming SSLv3 sessions.
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS_AES_128_GCM_SHA256
- 0x13,0x02 TLS_AES_256_GCM_SHA384
- 0x13,0x03 TLS_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2022/04/06

Plugin Output

tcp/443

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  Low Strength Ciphers (<= 64-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14        DH(512)       RSA      DES-CBC(40)
SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15        DH            RSA      DES-CBC(56)
SHA1
    EXP-ADH-DES-CBC-SHA           0x00, 0x19        DH(512)       None     DES-CBC(40)
SHA1      export
    EXP-ADH-RC4-MD5               0x00, 0x17        DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA               0x00, 0x1A        DH            None     DES-CBC(56)
SHA1
    EXP1024-DES-CBC-SHA           0x00, 0x62        RSA(1024)     RSA      DES-CBC(56)
SHA1      export
    EXP1024-RC2-CBC-MD5           0x00, 0x61        RSA(1024)     RSA      RC2-CBC(56)            MD5
       export
    EXP1024-RC4-MD5               0x00, 0x60        RSA(1024)     RSA      RC4(56)                MD5
       export
    EXP1024-RC4-SHA               0x00, 0x64        RSA(1024)     RSA      RC4(56)
SHA1      export
    DES-CBC-SHA                   0x00, 0x09        RSA           RSA      DES-CBC(56)
SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
SHA1
    ADH-DES-CBC3-SHA              0x00, 0x1B        DH            None     3DES-CBC(168)
SHA1
    DES-CBC3-SHA                  0x00, 0x0A        RSA           RSA      3DES-CBC(168)
SHA1

  High Strength Ciph [...]
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS_AES_128_GCM_SHA256
- 0x13,0x02 TLS_AES_256_GCM_SHA384
- 0x13,0x03 TLS_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2022/04/06

Plugin Output

tcp/5003

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  Low Strength Ciphers (<= 64-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14        DH(512)       RSA      DES-CBC(40)
SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15        DH            RSA      DES-CBC(56)
SHA1
    EXP-ADH-DES-CBC-SHA           0x00, 0x19        DH(512)       None     DES-CBC(40)
SHA1      export
    EXP-ADH-RC4-MD5               0x00, 0x17        DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA               0x00, 0x1A        DH            None     DES-CBC(56)
SHA1
    EXP1024-DES-CBC-SHA           0x00, 0x62        RSA(1024)     RSA      DES-CBC(56)
SHA1      export
    EXP1024-RC2-CBC-MD5           0x00, 0x61        RSA(1024)     RSA      RC2-CBC(56)            MD5
       export
    EXP1024-RC4-MD5               0x00, 0x60        RSA(1024)     RSA      RC4(56)                MD5
       export
    EXP1024-RC4-SHA               0x00, 0x64        RSA(1024)     RSA      RC4(56)
SHA1      export
    DES-CBC-SHA                   0x00, 0x09        RSA           RSA      DES-CBC(56)
SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
SHA1
    ADH-DES-CBC3-SHA              0x00, 0x1B        DH            None     3DES-CBC(168)
SHA1
    DES-CBC3-SHA                  0x00, 0x0A        RSA           RSA      3DES-CBC(168)
SHA1

  High Strength Ciph [...]
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS_AES_128_GCM_SHA256
- 0x13,0x02 TLS_AES_256_GCM_SHA384
- 0x13,0x03 TLS_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2022/04/06

Plugin Output

tcp/54345/loadrunner_agent

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  Low Strength Ciphers (<= 64-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14        DH(512)       RSA      DES-CBC(40)
SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15        DH            RSA      DES-CBC(56)
SHA1
    EXP-ADH-DES-CBC-SHA           0x00, 0x19        DH(512)       None     DES-CBC(40)
SHA1      export
    EXP-ADH-RC4-MD5               0x00, 0x17        DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA               0x00, 0x1A        DH            None     DES-CBC(56)
SHA1
    EXP1024-DES-CBC-SHA           0x00, 0x62        RSA(1024)     RSA      DES-CBC(56)
SHA1      export
    EXP1024-RC2-CBC-MD5           0x00, 0x61        RSA(1024)     RSA      RC2-CBC(56)            MD5
       export
    EXP1024-RC4-MD5               0x00, 0x60        RSA(1024)     RSA      RC4(56)                MD5
       export
    EXP1024-RC4-SHA               0x00, 0x64        RSA(1024)     RSA      RC4(56)
SHA1      export
    DES-CBC-SHA                   0x00, 0x09        RSA           RSA      DES-CBC(56)
SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
SHA1
    ADH-DES-CBC3-SHA              0x00, 0x1B        DH            None     3DES-CBC(168)
SHA1
    DES-CBC3-SHA                  0x00, 0x0A        RSA           RSA      3DES-CBC(168)
SHA1

  High Strength Ciph [...]
```

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
The remote host supports SMBv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2022/07/26

Plugin Output

tcp/443

```
An SSLv3 server answered on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2022/07/26

Plugin Output

tcp/2869/www

```
A web server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2022/07/26

Plugin Output

tcp/5003

```
An SSLv3 server answered on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2022/07/26

Plugin Output

tcp/8080/www

```
A web server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2022/07/26

Plugin Output

tcp/54345/loadrunner_agent

```
An SSLv3 server answered on this port.
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

tcp/0

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2021/11/19

Plugin Output

tcp/0

```
SMB was detected on port 445 but no credentials were provided.
SMB local checks were not enabled.
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.0.107 to 192.168.0.101 :
192.168.0.107
192.168.0.101

Hop Count: 1
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

135860 - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2022/08/15

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 3 NetBIOS names have been gathered :

 HHHTESTSERVER    = Computer name
 HHHTESTSERVER    = File Server Service
 WORKGROUP        = Workgroup / Domain name

The remote host has the following MAC address on its adapter :

   00:0c:29:bb:80:80
```