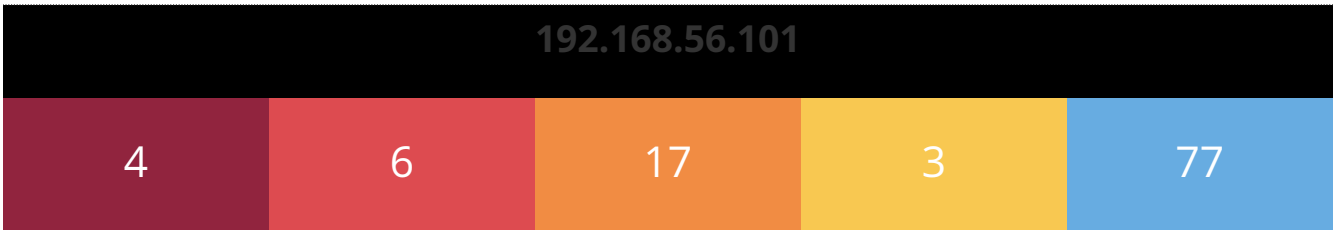
boot2root

Report generated by Nessus™ Thu, 06 Oct 2022 14:04:43 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host



Scan Information

Start time: Thu Oct 6 13:47:40 2022
End time: Thu Oct 6 14:04:42 2022

Host Information

IP: 192.168.56.101
MAC Address: 08:00:27:23:90:92
OS: Linux Kernel 3.0 on Ubuntu 12.04 (precise)

Vulnerabilities

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/143/imap

```
- 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


  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
    DES-CBC3-SHA                                   RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
```

```
   DHE-RSA-AES128-SHA                      DH             RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA                      DH             RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA                 DH             RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA                 DH             RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-SEED-SHA                        DH             RSA      SEED-CBC(128)
SHA1
   AES128-SHA                              RSA            RSA      AES-CBC(128)
SHA1
   AES256-SHA                              RSA            RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA                         RSA            RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA                         RSA            RSA      Camellia-CBC(256)
SHA1
   RC4-MD5                                 RSA            RSA      RC4(128)              MD5
   RC4-SHA                                 RSA            RSA      RC4(128)
SHA1
   SEED-SHA                                RSA            RSA       [...]
```

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/www

```
- 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


  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
    ECDHE-RSA-DES-CBC3-SHA                         ECDH          RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                                   RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    DHE-RSA-AES128-SHA                             DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA                             DH            RSA      AES-CBC(256)
 SHA1
    DHE-RSA-CAMELLIA128-SHA                        DH            RSA      Camellia-CBC(128)
 SHA1
    DHE-RSA-CAMELLIA256-SHA                        DH            RSA      Camellia-CBC(256)
 SHA1
    DHE-RSA-SEED-SHA                               DH            RSA      SEED-CBC(128)
 SHA1
    ECDHE-RSA-AES128-SHA                           ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA                           ECDH          RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-RC4-SHA                              ECDH          RSA      RC4(128)
 SHA1
    AES128-SHA                                     RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                                     RSA           RSA      AES-CBC(256)
 SHA1
    CAMELLIA128-SHA                                RSA           RSA      [...]
```

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/993/imap

```
- 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


  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
    DES-CBC3-SHA                                   RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    DHE-RSA-AES128-SHA                             DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA                             DH            RSA      AES-CBC(256)
 SHA1
    DHE-RSA-CAMELLIA128-SHA                        DH            RSA      Camellia-CBC(128)
 SHA1
    DHE-RSA-CAMELLIA256-SHA                        DH            RSA      Camellia-CBC(256)
 SHA1
    DHE-RSA-SEED-SHA                               DH            RSA      SEED-CBC(128)
 SHA1
    AES128-SHA                                     RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                                     RSA           RSA      AES-CBC(256)
 SHA1
    CAMELLIA128-SHA                                RSA           RSA      Camellia-CBC(128)
 SHA1
    CAMELLIA256-SHA                                RSA           RSA      Camellia-CBC(256)
 SHA1
    RC4-MD5                                        RSA           RSA      RC4(128)               MD5
    RC4-SHA                                        RSA           RSA      RC4(128)
 SHA1
    SEED-SHA                                       RSA           RSA       [...]
```

33850 - Unix Operating System Unsupported Version Detection

Synopsis

The operating system running on the remote host is no longer supported.

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

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.

Solution

Upgrade to a version of the Unix operating system 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 v2.0 Base Score

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

References

XREF	IAVA:0001-A-0502
XREF	IAVA:0001-A-0648

Plugin Information

Published: 2008/08/08, Modified: 2022/10/05

Plugin Output

tcp/0

```
Ubuntu 12.04 support ended on 2017-04-30.
Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04.

For more information, see : https://wiki.ubuntu.com/Releases
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

http://www.nessus.org/u?e120eea1

http://www.nessus.org/u?5d894816

http://www.nessus.org/u?51db68aa

http://www.nessus.org/u?9dc7bfba

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/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

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

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2009/01/05, Modified: 2022/01/14

Plugin Output

tcp/143/imap

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

Subject             : O=Dovecot mail server/OU=localhost/CN=localhost/E=root@mail.borntosec.net
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Oct 08 20:57:30 2015 GMT
Valid To            : Oct 07 20:57:30 2025 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIJAN968TzwGVlvMA0GCSqGSIb3DQEBBQUAMG4xHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxEjAQBgNVBAsMCWxvY2
+oKwqvb4Uc6CEHzrY4z/zG/HsZ/
cgNLgYkLevEf0+DIPliYSGo7yht28wbyW1GZGBvh5wYBRfJm8BDc5iyyuayQGxAOKXmgycv58jVvr4kuF0P0xW5vBHxzfDF1AXB2qNKg1h5oc6My1c
G+My8U5kQfSkL5OnKZ5Z1+pY3L9PzpNM6RJmx53ffi9jBlHnQ+TVTOzx72nqyKgR/at5P/
O4WSxxMztVY6d8ejaA0MQEcIjEQdTXFyCnfj1mHXRHpHaCQ6iVvkbJwJmKEWVXjcERoIVMik7zn4hMCAwEAAaNQME4wHQYDVR0OBBYEFA4UxwArd2v
+nw95NnON/RZrjEkEr24HAFJxn1zXgjEhlYToJgTNTCGLpOKr0weFEJcTiZLNuh7v++WLIM5YBpwscnbxL
+2ak9PLbGGVyq+RrX3RTzD5t6WZChwxCPqcNORB9pQknO9a7qG9kpl0ljGwg/xYvY+tETYBSz88Wy053Dq
+4on5tzkeLOxVi1WSA3XxdbQrS5kmfGCCIViPhl8QItIxBdZGoOY2niOszqDU4gaqKsx7wcIsDcKoXl2lNutwV8Eb/
HLBo8KBXjru3axYWy9JvJQkowL0Z5oHss3a2J3ErljjQLUlUFR6sd+tz0=
-----END CERTIFICATE-----
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

http://www.nessus.org/u?e120eea1

http://www.nessus.org/u?5d894816

http://www.nessus.org/u?51db68aa

http://www.nessus.org/u?9dc7bfba

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/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

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

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2009/01/05, Modified: 2022/01/14

Plugin Output

tcp/443/www

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

Subject             : CN=BornToSec
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Oct 08 00:19:46 2015 GMT
Valid To            : Oct 05 00:19:46 2025 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIICpDCCAYwCCQDVG5xgrjCJoDANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDEwlCb3JuVG9TZWMwHhcNMTUxMDA4MDAxOTQ2WhcNMjUxMDA1MDAxOT
Jw6py+3avYfKFCeRqHbOz/NxkBBRFXKDSwBX7z9+yDjjISbFZsb7Oc4q0M3MirRvivV7RXsv9oy5+TwVOG3pryK/SQVyaTR5auY/
omHN4sV283ieBwGDVujf2vdzj0BzfZr7Pwpp
+iCx6vGXVhwuEVwP3Ao8SVckMc0xXERyYQSgA9rl7OJ3hKswfzqhp6VuJMIOe38QD2Hmj4S/
SAnC8X5MWwspI5ZSyU7YF3aKpuEzpBCkU7nQr6eFU9nq6c7/u3vrs5GAjOVjJ4v32j
+yC9kwAPy0s756SHDobaguVYx9IasddKjVoFa
+wy0zMeEEGztAgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAJrrrBK9y1dzSG5vLml0PrZR66L
+lHCYpz/hSmmV2DyeYtRcZ5yl0qxBCtT5L0L/e2PGdXegQz/AL99S3zhfSkB
+tF9iTEx6RfInG7SvYlaDrMdilCRsto8VDad4NXNq8+hJRqkpTRoOhEPe/J+lVgUcekcUFgQ1c
+gpRtMdzci11hRdTapLL8Ve/8SCVuTVK3LL/sZ0Oz8ll+Gvvh/7EZ7DylyPNH1vq7MZvy
+cpEadrimGX10dKXiYfhUFbnq3bd0ZXGHKT1iAJGtUfQ7nNuJ8R5MaPr+73mhbV4wwcmaDz1e66XUi9EcvSWvAe
+zSy93YwsV1eX91FU56FFipSCQ=
-----END CERTIFICATE-----
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

http://www.nessus.org/u?e120eea1

http://www.nessus.org/u?5d894816

http://www.nessus.org/u?51db68aa

http://www.nessus.org/u?9dc7bfba

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/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

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

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2009/01/05, Modified: 2022/01/14

Plugin Output

tcp/993/imap

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

Subject             : O=Dovecot mail server/OU=localhost/CN=localhost/E=root@mail.borntosec.net
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Oct 08 20:57:30 2015 GMT
Valid To            : Oct 07 20:57:30 2025 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIJAN968TzwGVlvMA0GCSqGSIb3DQEBBQUAMG4xHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxEjAQBgNVBAsMCWxvY2
+oKwqvb4Uc6CEHzrY4z/zG/HsZ/
cgNLgYkLevEf0+DIPliYSGo7yht28wbyW1GZGBvh5wYBRfJm8BDc5iyyuayQGxAOKXmgycv58jVvr4kuF0P0xW5vBHxzfDF1AXB2qNKg1h5oc6My1c
G+My8U5kQfSkL5OnKZ5Z1+pY3L9PzpNM6RJmx53ffi9jBlHnQ+TVTOzx72nqyKgR/at5P/
O4WSxxMztVY6d8ejaA0MQEcIjEQdTXFyCnfj1mHXRHpHaCQ6iVvkbJwJmKEWVXjcERoIVMik7zn4hMCAwEAAaNQME4wHQYDVR0OBBYEFA4UxwArd2v
+nw95NnON/RZrjEkEr24HAFJxn1zXgjEhlYToJgTNTCGLpOKr0weFEJcTiZLNuh7v++WLIM5YBpwscnbxL
+2ak9PLbGGVyq+RrX3RTzD5t6WZChwxCPqcNORB9pQknO9a7qG9kpl0ljGwg/xYvY+tETYBSz88Wy053Dq
+4on5tzkeLOxVi1WSA3XxdbQrS5kmfGCCIViPhl8QItIxBdZGoOY2niOszqDU4gaqKsx7wcIsDcKoXl2lNutwV8Eb/
HLBo8KBXjru3axYWy9JvJQkowL0Z5oHss3a2J3ErljjQLUlUFR6sd+tz0=
-----END CERTIFICATE-----
```

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/143/imap

```
  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
    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/443/www

```
  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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      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/993/imap

```
  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
    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}
```

88098 - Apache Server ETag Header Information Disclosure

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

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 v3.0 Temporal Score

4.6 (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	6939
CVE	CVE-2003-1418
XREF	CWE:200

Plugin Information

Published: 2016/01/22, Modified: 2020/04/27

Plugin Output

tcp/80/www

```
Nessus was able to determine that the Apache Server listening on
port 80 leaks the servers inode numbers in the ETag HTTP
Header field :

  Source                 : ETag: "3552-401-5218c3c475880"
  Inode number           : 13650
  File size              : 1025 bytes
  File modification time : Oct.  7, 2015 at 23:37:54 GMT
```

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

https://tools.ietf.org/html/rfc4253#section-6.3

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

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: 2016/04/04, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following weak server-to-client encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256

The following weak client-to-server encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256
```

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/143/imap

```
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 : O=Dovecot mail server/OU=localhost/CN=localhost/E=root@mail.borntosec.net
|-Issuer  : O=Dovecot mail server/OU=localhost/CN=localhost/E=root@mail.borntosec.net
```

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/www

```
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 : CN=BornToSec
|-Issuer  : CN=BornToSec
```

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/993/imap

```
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 : O=Dovecot mail server/OU=localhost/CN=localhost/E=root@mail.borntosec.net
|-Issuer  : O=Dovecot mail server/OU=localhost/CN=localhost/E=root@mail.borntosec.net
```

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/143/imap

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    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/443/www

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     --------------------   ---
    ECDHE-RSA-RC4-SHA             0xC0, 0x11        ECDH          RSA      RC4(128)
 SHA1
    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/993/imap

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    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/143/imap

```
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 : O=Dovecot mail server/OU=localhost/CN=localhost/E=root@mail.borntosec.net
```

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/www

```
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 : CN=BornToSec
```

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/993/imap

```
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 : O=Dovecot mail server/OU=localhost/CN=localhost/E=root@mail.borntosec.net
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/143/imap

```
TLSv1 is enabled and the server supports at least one cipher.
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/443/www

```
TLSv1 is enabled and the server supports at least one cipher.
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/993/imap

```
TLSv1 is enabled and the server supports at least one cipher.
```

157288 - TLS Version 1.1 Protocol Deprecated

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://datatracker.ietf.org/doc/html/rfc8996

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2022/04/04, Modified: 2022/04/11

Plugin Output

tcp/143/imap

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

157288 - TLS Version 1.1 Protocol Deprecated

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://datatracker.ietf.org/doc/html/rfc8996

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2022/04/04, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

157288 - TLS Version 1.1 Protocol Deprecated

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://datatracker.ietf.org/doc/html/rfc8996

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2022/04/04, Modified: 2022/04/11

Plugin Output

tcp/993/imap

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

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	32319
CVE	CVE-2008-5161
XREF	CERT:958563
XREF	CWE:200

Plugin Information

Published: 2013/10/28, Modified: 2018/07/30

Plugin Output

tcp/22/ssh

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :
```

```
  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

153953 - SSH Weak Key Exchange Algorithms Enabled

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

See Also

http://www.nessus.org/u?b02d91cd

https://datatracker.ietf.org/doc/html/rfc8732

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2021/10/13, Modified: 2021/10/13

Plugin Output

tcp/22/ssh

```
The following weak key exchange algorithms are enabled :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group1-sha1
```

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

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

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

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: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
  hmac-sha2-256-96
  hmac-sha2-512-96

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
  hmac-sha2-256-96
  hmac-sha2-512-96
```

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2022/03/21

Plugin Output

tcp/0

```
The Linux distribution detected was :
 - Ubuntu 12.04 (precise)
 - Ubuntu 12.10 (quantal)
 - Ubuntu 13.04 (raring)
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2022/09/08

Plugin Output

tcp/80/www

```
URL        : http://192.168.56.101/
Version    : 2.2.99
Source     : Server: Apache/2.2.22 (Ubuntu)
backported : 1
os         : ConvertedUbuntu
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2022/09/08

Plugin Output

tcp/443/www

```
URL        : https://192.168.56.101/
Version    : 2.2.99
Source     : Server: Apache/2.2.22 (Ubuntu)
backported : 1
os         : ConvertedUbuntu
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Give Nessus credentials to perform local checks.
```

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/80/www

```
Give Nessus credentials to perform local checks.
```

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/443/www

```
Give Nessus credentials to perform local checks.
```

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: 2022/10/05

Plugin Output

tcp/0

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

  cpe:/o:canonical:ubuntu_linux:12.04 -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.2.22 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apache:http_server:2.2.99 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:openbsd:openssh:5.9 -> OpenBSD OpenSSH
```

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: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 95
```

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 :

08:00:27:23:90:92 : PCS Systemtechnik GmbH
```

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:
  - 08:00:27:23:90:92
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

tcp/21

```
The remote FTP banner is :
220 Welcome on this server
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/443/www

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

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/80/www

```
Based on the response to an OPTIONS request :
  - HTTP methods GET HEAD OPTIONS POST are allowed on :
    /
```

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/443/www

```
Based on the response to an OPTIONS request :
  - HTTP methods GET HEAD OPTIONS POST 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/80/www

```
The remote web server type is :

Apache/2.2.22 (Ubuntu)
```

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/443/www

```
The remote web server type is :

Apache/2.2.22 (Ubuntu)
```

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/80/www

```
Response Code : HTTP/1.1 200 OK

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

  Date: Thu, 06 Oct 2022 11:49:51 GMT
  Server: Apache/2.2.22 (Ubuntu)
  Last-Modified: Wed, 07 Oct 2015 23:37:54 GMT
  ETag: "3552-401-5218c3c475880"
  Accept-Ranges: bytes
  Content-Length: 1025
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Hack me if you can</title>
<meta name='description' content='Simple and clean HTML coming soon / under construction page'/>
```

```
<meta name='keywords' content='coming soon, html, html5, css3, css, under construction'/>
<link rel="stylesheet" href="style.css" type="text/css" media="screen, projection" />
<link href='http://fonts.googleapis.com/css?family=Coustard' rel='stylesheet' type='text/css'>
</head>
<body>
<div id="wrapper">
<h1>Hack me</h1>
<h2>We're Coming Soon</h2>
<p>We're wetting our shirts to launch the website.<br />
In the mean time, you can connect with us trought</p>
<p><a href="https://fr-fr.facebook.com/42Born2Code"><img src="fb.png" alt="Facebook" /></a>
 <a href="https://plus.google.com/+42Frborn2code"><img src="+.png" alt="Google +" /></a> <a
 href="https://twitter.com/42born2code"><img src="twitter.png" alt="Twitter" /></a></p>
</div>
</body>
</html>
```

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/443/www

```
Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Thu, 06 Oct 2022 11:49:51 GMT
  Server: Apache/2.2.22 (Ubuntu)
  Vary: Accept-Encoding
  Content-Length: 279
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=iso-8859-1

Response Body :
```

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 difference between the local and remote clocks is -5 seconds.
```

11414 - IMAP Service Banner Retrieval

Synopsis

An IMAP server is running on the remote host.

Description

An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/03/18, Modified: 2011/03/16

Plugin Output

tcp/143/imap

```
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS LOGINDISABLED]
 Dovecot ready.
```

11414 - IMAP Service Banner Retrieval

Synopsis

An IMAP server is running on the remote host.

Description

An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/03/18, Modified: 2011/03/16

Plugin Output

tcp/993/imap

```
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot
 ready.
```

42085 - IMAP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote IMAP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS

https://tools.ietf.org/html/rfc2595

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2021/02/24

Plugin Output

tcp/143/imap

```
Here is the IMAP server's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

------------------------------ snip ------------------------------
Subject Name:

Organization: Dovecot mail server
Organization Unit: localhost
Common Name: localhost
Email Address: root@mail.borntosec.net

Issuer Name:

Organization: Dovecot mail server
Organization Unit: localhost
Common Name: localhost
Email Address: root@mail.borntosec.net

Serial Number: 00 DF 7A F1 3C F0 19 59 6F

Version: 3
```

```
Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 08 20:57:30 2015 GMT
Not Valid After: Oct 07 20:57:30 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 CA 63 3D 0D 88 E9 89 0D 8D 9A 71 90 48 DF C3 B5 F1 66 1A
            FE A0 AC 2A BD BE 14 73 A0 84 1F 3A D8 E3 3F F3 1B F1 EC 67
            F7 20 34 B8 18 90 B7 AF 11 FD 3E 0C 83 E5 89 84 86 A3 BC A1
            B7 6F 30 6F 25 B5 19 91 81 BE 1E 70 60 14 5F 26 6F 01 0D CE
            62 CB 2B 9A C9 01 B1 00 E2 97 9A 0C 9C BF 9F 23 56 FA F8 92
            E1 74 3F 4C 56 E6 F0 47 C7 37 C3 17 50 17 07 6A 8D 2A 0D 61
            E6 87 3A 33 2D 68 C7 A1 3C 4C 74 B1 52 B0 B0 CC 6D 9B E0 8F
            2A 76 98 80 90 8F C6 F8 CC BC 53 99 10 7D 29 0B E4 E9 CA 67
            96 75 FA 96 37 2F D3 F3 A4 D3 3A 44 99 B1 E7 77 DF 8B D8 C1
            94 79 D0 F9 35 53 3B 3C 7B DA 7A B2 2A 04 7F 6A DE 4F FC EE
            16 4B 1C 4C CE D5 58 E9 DF 1E 8D A0 34 31 01 1C 22 31 10 75
            35 C5 C8 29 DF 8F 59 87 5D 11 E9 1D A0 90 EA 25 6F 91 B2 70
            26 62 84 59 55 E3 70 44 68 21 53 22 93 BC E7 E2 13
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 AB A8 3A 42 41 4C 31 63 13 A6 B4 EB A0 8F 5D 0E AE 94 4E
           AC 88 DD 41 FA 7C 3D E4 D9 CE 37 F4 59 AE 31 24 12 BD B8 1C
           01 49 C6 7D 73 5E 08 C4 86 56 13 A0 98 13 35 30 86 2E 93 8A
           AF 4C 1E 14 42 5C 4E 26 4B 36 E8 7B BF EF 96 2C 83 39 60 1A
           70 B1 C9 DB C4 BF B6 6A 4F 4F [...]
```

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/21

```
Port 21/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/22/ssh

```
Port 22/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/80/www

```
Port 80/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/143/imap

```
Port 143/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/www

```
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/993/imap

```
Port 993/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 : 202210060545
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : fc34-x86-64
Scan type : Normal
Scan name : boot2root
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.56.1
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 86.440 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 : Detected
Allow post-scan editing : Yes
Scan Start Date : 2022/10/6 13:47 CEST
Scan duration : 1018 sec
```

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 : Linux Kernel 3.0 on Ubuntu 12.04 (precise)
Confidence level : 95
Method : SSH


The remote host is running Linux Kernel 3.0 on Ubuntu 12.04 (precise)
```

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 SSH 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 143 was detected as being open but is now closed
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/143/imap

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/443/www

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/993/imap

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  ssh-dss
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
```

```
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha2-256
  hmac-sha2-256-96
  hmac-sha2-512
  hmac-sha2-512-96
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha2-256
  hmac-sha2-256-96
  hmac-sha2-512
  hmac-sha2-512-96
  umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2021/01/19

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-96

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-96
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.7
SSH supported authentication : publickey,password
SSH banner :
        _____                 _______    _____
       |  _ \               |__   __|  / ____|
       | |_) | ___  _ __ _ __ | | ___| (___   ___  ___
       |  _ < / _ \| '__| '_ \| |/ _ \\___ \ / _ \/ __|
       | |_) | (_) | |  | | | | | (_) |___) |  __/ (__
       |____/ \___/|_|  |_| |_|_|\___/_____/ \___|\___|

                        Good luck & Have fun
```

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/143/imap

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

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/www

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

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/993/imap

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

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/143/imap

```
Subject Name:

Organization: Dovecot mail server
Organization Unit: localhost
Common Name: localhost
Email Address: root@mail.borntosec.net

Issuer Name:

Organization: Dovecot mail server
Organization Unit: localhost
Common Name: localhost
Email Address: root@mail.borntosec.net

Serial Number: 00 DF 7A F1 3C F0 19 59 6F

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 08 20:57:30 2015 GMT
Not Valid After: Oct 07 20:57:30 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 CA 63 3D 0D 88 E9 89 0D 8D 9A 71 90 48 DF C3 B5 F1 66 1A
            FE A0 AC 2A BD BE 14 73 A0 84 1F 3A D8 E3 3F F3 1B F1 EC 67
            F7 20 34 B8 18 90 B7 AF 11 FD 3E 0C 83 E5 89 84 86 A3 BC A1
            B7 6F 30 6F 25 B5 19 91 81 BE 1E 70 60 14 5F 26 6F 01 0D CE
            62 CB 2B 9A C9 01 B1 00 E2 97 9A 0C 9C BF 9F 23 56 FA F8 92
```

```
             E1 74 3F 4C 56 E6 F0 47 C7 37 C3 17 50 17 07 6A 8D 2A 0D 61
             E6 87 3A 33 2D 68 C7 A1 3C 4C 74 B1 52 B0 B0 CC 6D 9B E0 8F
             2A 76 98 80 90 8F C6 F8 CC BC 53 99 10 7D 29 0B E4 E9 CA 67
             96 75 FA 96 37 2F D3 F3 A4 D3 3A 44 99 B1 E7 77 DF 8B D8 C1
             94 79 D0 F9 35 53 3B 3C 7B DA 7A B2 2A 04 7F 6A DE 4F FC EE
             16 4B 1C 4C CE D5 58 E9 DF 1E 8D A0 34 31 01 1C 22 31 10 75
             35 C5 C8 29 DF 8F 59 87 5D 11 E9 1D A0 90 EA 25 6F 91 B2 70
             26 62 84 59 55 E3 70 44 68 21 53 22 93 BC E7 E2 13
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 AB A8 3A 42 41 4C 31 63 13 A6 B4 EB A0 8F 5D 0E AE 94 4E
           AC 88 DD 41 FA 7C 3D E4 D9 CE 37 F4 59 AE 31 24 12 BD B8 1C
           01 49 C6 7D 73 5E 08 C4 86 56 13 A0 98 13 35 30 86 2E 93 8A
           AF 4C 1E 14 42 5C 4E 26 4B 36 E8 7B BF EF 96 2C 83 39 60 1A
           70 B1 C9 DB C4 BF B6 6A 4F 4F 2D B1 86 57 2A BE 46 B5 F7 45
           3C C3 E6 DE 96 64 28 70 C4 23 EA 70 D3 91 07 DA 50 92 73 BD
           6B BA 86 F6 4A 65 D2 58 C6 C2 0F F1 62 F6 3E B4 44 D8 05 2C
     [...]
```

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/www

```
Subject Name:

Common Name: BornToSec

Issuer Name:

Common Name: BornToSec

Serial Number: 00 D5 1B 9C 60 AE 30 89 A0

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 08 00:19:46 2015 GMT
Not Valid After: Oct 05 00:19:46 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BC D4 28 67 23 46 78 71 A9 4C E4 34 1C FC 9C 3A A7 2F B7
            6A F6 1F 28 50 9E 46 A1 DB 3B 3F CD C6 40 41 44 55 CA 0D 2C
            01 5F BC FD FB 20 E3 8C 84 9B 15 9B 1B EC E7 38 AB 43 37 32
            2A D1 BE 2B D5 ED 15 EC BF DA 32 E7 E4 F0 54 E1 B7 A6 BC 8A
            FD 24 15 C9 A4 D1 E5 AB 98 FE 89 87 37 8B 15 DB CD E2 78 1C
            06 0D 5B A3 7F 6B DD CE 3D 01 CD F6 6B EC FC 29 A7 E8 82 C7
            AB C6 5D 58 70 B8 45 70 3F 70 28 F1 25 5C 90 C7 34 C5 71 11
            C9 84 12 80 0F 6B 97 B3 89 DE 12 AC C1 FC EA 86 9E 95 B8 93
            08 39 ED FC 40 3D 87 9A 3E 12 FD 20 27 0B C5 F9 31 6C 2C A4
            8E 59 4B 25 3B 60 5D DA 2A 9B 84 CE 90 42 91 4E E7 42 BE 9E
            15 4F 67 AB A7 3B FE ED EF AE CE 46 02 33 95 8C 9E 2F DF 68
```

```
             FE C8 2F 64 C0 03 F2 D2 CE F9 E9 21 C3 A1 B6 A0 B9 56 31 F4
             86 AC 75 D2 A3 56 81 5A FB 0C B4 CC C7 84 10 6C ED
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 9A EB AC 12 BD CB 57 73 48 6E 6F 2E 69 74 3E B6 51 EB A2
           FE 94 70 98 A7 3F E1 4A 69 95 D8 3C 9E 62 D4 5C 67 9C A5 D2
           AC 41 0A D4 F9 2F 42 FF 7B 63 C6 75 77 A0 43 3F C0 2F DF 52
           DF 38 5F 4A 40 7E B4 5F 62 4C 4C 7A 45 F2 27 1B B4 AF 62 56
           83 AC C7 62 94 24 6C B6 8F 15 0D A7 78 35 73 6A F3 E8 49 46
           A9 29 4D 1A 0E 84 43 DE FC 9F A5 56 05 1C 7A 47 14 16 04 35
           73 E8 29 46 D3 1D CD C8 B5 D6 14 5D 4D AA 4B 2F C5 5E FF C4
           82 56 E4 D5 2B 72 CB FE C6 74 3B 3F 25 97 E1 AF BE 1F FB 11
           9E C3 CA 5C 8F 34 7D 6F AB B3 19 BF 2F 9C A4 46 9D AE 29 86
           5F 5D 1D 29 78 98 7E 15 05 6E 7A B7 6D DD 19 5C 61 CA [...]
```

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/993/imap

```
Subject Name:

Organization: Dovecot mail server
Organization Unit: localhost
Common Name: localhost
Email Address: root@mail.borntosec.net

Issuer Name:

Organization: Dovecot mail server
Organization Unit: localhost
Common Name: localhost
Email Address: root@mail.borntosec.net

Serial Number: 00 DF 7A F1 3C F0 19 59 6F

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 08 20:57:30 2015 GMT
Not Valid After: Oct 07 20:57:30 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 CA 63 3D 0D 88 E9 89 0D 8D 9A 71 90 48 DF C3 B5 F1 66 1A
            FE A0 AC 2A BD BE 14 73 A0 84 1F 3A D8 E3 3F F3 1B F1 EC 67
            F7 20 34 B8 18 90 B7 AF 11 FD 3E 0C 83 E5 89 84 86 A3 BC A1
            B7 6F 30 6F 25 B5 19 91 81 BE 1E 70 60 14 5F 26 6F 01 0D CE
            62 CB 2B 9A C9 01 B1 00 E2 97 9A 0C 9C BF 9F 23 56 FA F8 92
```

```
             E1 74 3F 4C 56 E6 F0 47 C7 37 C3 17 50 17 07 6A 8D 2A 0D 61
             E6 87 3A 33 2D 68 C7 A1 3C 4C 74 B1 52 B0 B0 CC 6D 9B E0 8F
             2A 76 98 80 90 8F C6 F8 CC BC 53 99 10 7D 29 0B E4 E9 CA 67
             96 75 FA 96 37 2F D3 F3 A4 D3 3A 44 99 B1 E7 77 DF 8B D8 C1
             94 79 D0 F9 35 53 3B 3C 7B DA 7A B2 2A 04 7F 6A DE 4F FC EE
             16 4B 1C 4C CE D5 58 E9 DF 1E 8D A0 34 31 01 1C 22 31 10 75
             35 C5 C8 29 DF 8F 59 87 5D 11 E9 1D A0 90 EA 25 6F 91 B2 70
             26 62 84 59 55 E3 70 44 68 21 53 22 93 BC E7 E2 13
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 AB A8 3A 42 41 4C 31 63 13 A6 B4 EB A0 8F 5D 0E AE 94 4E
           AC 88 DD 41 FA 7C 3D E4 D9 CE 37 F4 59 AE 31 24 12 BD B8 1C
           01 49 C6 7D 73 5E 08 C4 86 56 13 A0 98 13 35 30 86 2E 93 8A
           AF 4C 1E 14 42 5C 4E 26 4B 36 E8 7B BF EF 96 2C 83 39 60 1A
           70 B1 C9 DB C4 BF B6 6A 4F 4F 2D B1 86 57 2A BE 46 B5 F7 45
           3C C3 E6 DE 96 64 28 70 C4 23 EA 70 D3 91 07 DA 50 92 73 BD
           6B BA 86 F6 4A 65 D2 58 C6 C2 0F F1 62 F6 3E B4 44 D8 05 2C
     [...]
```

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/143/imap

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

  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
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
```

```
   DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH            RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH            RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA               0x00, 0x41       RSA           RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA               0x00, 0x84       RSA           RSA      Camellia-CBC(256)
SHA1
   SEED-SHA                      0x00, 0x96       RSA           RSA      SEED-CBC(128)
SHA1
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
SHA256
   RSA-AES128-SHA256              [...]
```

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/www

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

  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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      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
    ----------------------        ----------       ---           ----     ---------------------  ---
```

```
   DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH            RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH            RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA               0x00, 0x41       RSA           RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA               0x00, 0x84       RSA           RSA      Camellia-CBC(256)
SHA1
   SEED-SHA                      0x00 [...]
```

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/993/imap

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

  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
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
```

```
   DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH            RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH            RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA               0x00, 0x41       RSA           RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA               0x00, 0x84       RSA           RSA      Camellia-CBC(256)
SHA1
   SEED-SHA                      0x00, 0x96       RSA           RSA      SEED-CBC(128)
SHA1
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
SHA256
   RSA-AES128-SHA256              [...]
```

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/143/imap

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  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
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
```

```
   RSA-AES256-SHA384            0x00, 0x9D      RSA           RSA      AES-GCM(256)
SHA384
   DHE-RSA-AES128-SHA           0x00, 0x33      DH            RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA           0x00, 0x39      DH            RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA      0x00, 0x45      DH            RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA      0x00, 0x88      DH            RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-SEED-SHA             0x00, 0x9A      DH            RSA      SEED-CBC(128)
SHA1
   AES128-SHA                   0x00, 0x2F      RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                   0x00, 0x35      RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA              0x00, 0x41      RSA           RSA      C [...]
```

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/www

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  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
    ECDHE-RSA-DES-CBC3-SHA       0xC0, 0x12       ECDH          RSA      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
    ----------------------       ----------       ---           ----     --------------------   ---
    DHE-RSA-AES128-SHA256        0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384        0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
```

```
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F      ECDH           RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30      ECDH           RSA      AES-GCM(256)
SHA384
   RSA-AES128-SHA256             0x00, 0x9C      RSA            RSA      AES-GCM(128)
SHA256
   RSA-AES256-SHA384             0x00, 0x9D      RSA            RSA      AES-GCM(256)
SHA384
   DHE-RSA-AES128-SHA            0x00, 0x33      DH             RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39      DH             RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45      DH             RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88      DH             RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-SEED-SHA              0x00, 0x9A      DH             RSA    [...]
```

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/993/imap

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  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
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
```

```
   RSA-AES256-SHA384            0x00, 0x9D      RSA           RSA      AES-GCM(256)
SHA384
   DHE-RSA-AES128-SHA           0x00, 0x33      DH            RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA           0x00, 0x39      DH            RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA      0x00, 0x45      DH            RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA      0x00, 0x88      DH            RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-SEED-SHA             0x00, 0x9A      DH            RSA      SEED-CBC(128)
SHA1
   AES128-SHA                   0x00, 0x2F      RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                   0x00, 0x35      RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA              0x00, 0x41      RSA           RSA      C [...]
```

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/143/imap

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

  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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
```

```
   DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH            RSA      Camellia-CBC(128)
 SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH            RSA      Camellia-CBC(256)
 SHA1
   DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
 SHA1
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256

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/443/www

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

  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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
```

```
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH           RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH         RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH         RSA      AES-GCM(256)
SHA384
   DHE-RSA-AES128-SHA            0x00, 0x33       DH           RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39       DH           RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH           RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH           RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-SEED-SHA              0x00, 0x9A       DH           RSA      SEED-CBC(128)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH         RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH         RSA      AES-CBC(256)
SHA1
   ECDHE-RSA-RC4-SHA             0xC0, 0x11       ECDH         RSA      RC4(128)
SHA1
   DHE-RSA-AES128-SHA256      [...]
```

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/993/imap

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

  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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
```

```
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH            RSA      Camellia-CBC(128)
 SHA1
    DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH            RSA      Camellia-CBC(256)
 SHA1
    DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256

The fields above are :

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

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/143/imap

```
The following root Certification Authority certificate was found :

|-Subject             : O=Dovecot mail server/OU=localhost/CN=localhost/E=root@mail.borntosec.net
|-Issuer              : O=Dovecot mail server/OU=localhost/CN=localhost/E=root@mail.borntosec.net
|-Valid From          : Oct 08 20:57:30 2015 GMT
|-Valid To            : Oct 07 20:57:30 2025 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/993/imap

```
The following root Certification Authority certificate was found :

|-Subject             : O=Dovecot mail server/OU=localhost/CN=localhost/E=root@mail.borntosec.net
|-Issuer              : O=Dovecot mail server/OU=localhost/CN=localhost/E=root@mail.borntosec.net
|-Valid From          : Oct 08 20:57:30 2015 GMT
|-Valid To            : Oct 07 20:57:30 2025 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

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/www

```
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/143/imap

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  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
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
SHA256
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH            RSA      Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH            RSA      Camellia-CBC(256)
SHA1
    DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
    CAMELLIA128-SHA               0x00, 0x41       RSA           RSA      Camellia-CBC(128)
SHA1
    CAMELLIA256-SHA               0x00, 0x84       RSA           RSA      Camellia-CBC(256)
SHA1
    RC4-MD5                       0x00, 0x04       RSA           RSA      RC4(128)               MD
[...]
```

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/www

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          RSA      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
    ----------------------        ----------        ---           ----     --------------------   ---
    RSA-AES128-SHA256             0x00, 0x9C        RSA           RSA      AES-GCM(128)
SHA256
    RSA-AES256-SHA384             0x00, 0x9D        RSA           RSA      AES-GCM(256)
SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45        DH            RSA      Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA       0x00, 0x88        DH            RSA      Camellia-CBC(256)
SHA1
    DHE-RSA-SEED-SHA              0x00, 0x9A        DH            RSA      SEED-CBC(128)
SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA      AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          RSA      AES-CBC(256)
SHA1
    ECDHE-RSA-RC4-SHA             0xC0, 0x11        ECDH          RSA      RC4(128)
SHA1
    AES128-SHA                    0x00, 0x2F        RSA           RSA      AES-CBC(128)           SH
[...]
```

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/993/imap

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  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
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
SHA256
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH            RSA      Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH            RSA      Camellia-CBC(256)
SHA1
    DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
    CAMELLIA128-SHA               0x00, 0x41       RSA           RSA      Camellia-CBC(128)
SHA1
    CAMELLIA256-SHA               0x00, 0x84       RSA           RSA      Camellia-CBC(256)
SHA1
    RC4-MD5                       0x00, 0x04       RSA           RSA      RC4(128)               MD
[...]
```

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/22/ssh

```
An SSH 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/80/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/143/imap

```
An IMAP 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/443/www

```
A TLSv1 server answered on this port.
```

tcp/443/www

```
A web server is running on this port through TLSv1.
```

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/993/imap

```
A TLSv1 server answered on this port.
```

tcp/993/imap

```
An IMAP server is running on this port through TLSv1.
```

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

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

tcp/143/imap

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

tcp/443/www

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

tcp/993/imap

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/143/imap

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/443/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/993/imap

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

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

```
SSH was detected on port 22 but no credentials were provided.
SSH 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 192.168.56.1 to 192.168.56.101 :
192.168.56.1
192.168.56.101

Hop Count: 1
```