facebookadvancedscan

Report generated by Nessus™ Thu, 02 Dec 2021 23:18:23 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

157.240.239.35

0	1	1	0	33
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Thu Dec 2 23:08:32 2021

End time: Thu Dec 2 23:18:23 2021

Host Information

DNS Name: edge-star-mini-shv-02-del1.facebook.com

IP: 157.240.239.35

OS: Ubuntu 14.04 Linux Kernel 3.13

Vulnerabilities

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
    ----------------------       ----------       ---           ----     ---------------------  ---
    ECDHE-ECDSA-DES-CBC3-SHA     0xC0, 0x08       ECDH          ECDSA    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}
```

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.
```

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

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

Solution

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information

Published: 2010/04/29, Modified: 2020/06/12

Plugin Output

tcp/0

```
The following hostnames point to the remote host :
  - facebook.com
  - ads.facebook.com
  - connect.facebook.com
```

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: 2021/11/29

Plugin Output

tcp/0

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

  cpe:/o:linux:linux_kernel:3.13
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Remote device type : unknown
Confidence level : 56
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
157.240.239.35 resolves as edge-star-mini-shv-02-del1.facebook.com.
```

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/1.1 301 Moved Permanently

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

  Location: https://edge-star-mini-shv-02-del1.facebook.com/
  Content-Type: text/html; charset="utf-8"
  X-FB-Debug: WcBfI+Ibwxe1PA2VgiztOvGx8I1CMgwGdrxF3JA7bjGM91hIQsxSVwC0/MgqGXBonfcgnE0WI7S5oJ+
+aamC6A==
  Date: Thu, 02 Dec 2021 17:46:28 GMT
  Priority: u=3,i
  Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600
  Connection: keep-alive
  Content-Length: 0

Response Body :
```

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/1.1 302 Found

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

  Location: https://m.facebook.com/?_rdr
  Strict-Transport-Security: max-age=15552000; preload
  Content-Type: text/html; charset="utf-8"
  X-FB-Debug: bko/Bl5I0qw3MUgoUaDoG/m99lX0TssztvrdPCR2dK/
i9Sy5jXEpdYQVAI5a0hEjMvTz9fl64sHUcF6+0o3fcg==
  Date: Thu, 02 Dec 2021 17:46:30 GMT
  Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600
  Connection: keep-alive
  Content-Length: 0

Response Body :
```

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: 2021/09/16

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: 2021/09/16

Plugin Output

tcp/443/www

```
Port 443/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: 2021/09/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.0.1
Nessus build : 20287
Plugin feed version : 202112020807
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : facebookadvancedscan
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.1.10
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 14.641 ms
Thorough tests : no
Experimental tests : 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 : 5
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/12/2 23:08 India Standard Time
Scan duration : 578 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: 2021/09/27

Plugin Output

tcp/0

```
Remote operating system : Ubuntu 14.04 Linux Kernel 3.13
Confidence level : 56
Method : MLSinFP


The remote host is running Ubuntu 14.04 Linux Kernel 3.13
```

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

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 TLSv1.3/TLSv1.0/TLSv1.1/TLSv1.2.
```

83298 - SSL Certificate Chain Contains Certificates Expiring Soon

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

Plugin Output

tcp/443/www

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject   : C=US/ST=California/L=Menlo Park/O=Facebook, Inc./CN=*.facebook.com
|-Not After : Dec 10 23:59:59 2021 GMT
```

42981 - SSL Certificate Expiry - Future Expiry

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

Solution

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

Risk Factor

None

Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

Plugin Output

tcp/443/www

```
The SSL certificate will expire within 60 days, at
Dec 10 23:59:59 2021 GMT :

  Subject          : C=US, ST=California, L=Menlo Park, O=Facebook, Inc., CN=*.facebook.com
  Issuer           : C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance
 Server CA
  Not valid before : Sep 11 00:00:00 2021 GMT
  Not valid after  : Dec 10 23:59:59 2021 GMT
```

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:

Country: US
State/Province: California
Locality: Menlo Park
Organization: Facebook, Inc.
Common Name: *.facebook.com

Issuer Name:

Country: US
Organization: DigiCert Inc
Organization Unit: www.digicert.com
Common Name: DigiCert SHA2 High Assurance Server CA

Serial Number: 01 EE 8A 59 7C 2B 93 74 77 E8 7E 33 04 7C 5C 3A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Sep 11 00:00:00 2021 GMT
Not Valid After: Dec 10 23:59:59 2021 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 70 A3 8F 4D A8 B2 9B 51 1E 02 EB 71 3E 74 F0 9B 62 C0 1D 73
              25 01 D0 E6 63 A6 58 4F 16 DD AF D2
Public Key Y: 80 4C 7A F1 04 54 C4 93 F3 D4 10 FA 8B DD 51 43 70 DB BC E9
```

```
               1F 01 29 BC 64 E4 75 21 CB 51 D2 29

Signature Length: 256 bytes / 2048 bits
Signature: 00 90 B5 C7 2C 1E 5C BB 51 DA 99 34 67 66 ED 2F 26 57 49 85
           E7 2D 20 EC D1 07 9E 37 72 53 C7 0F 7F C3 C5 3A 32 45 29 8C
           AE 37 75 C3 BE 02 AC A1 3D B1 B7 77 A5 7A 28 1B C6 59 C4 15
           0B D9 87 3E BE 3F 13 F5 47 B0 45 46 DB 66 B4 0E 8A 92 3D 2F
           38 5C 21 59 95 41 22 2D 96 05 1F 54 6E E0 E0 DA 95 7F B7 AA
           2C 31 2B 44 49 7B D2 3F 73 40 E1 D1 03 B3 89 D5 F9 B0 3F AA
           35 D4 04 D2 D4 56 53 D5 67 18 8E 80 C1 C3 16 89 FB 0C 60 91
           5A 12 EF EE D1 8B 4B 42 78 CF D5 27 4F 78 32 45 E3 09 75 21
           FD 11 80 1F 3C D9 87 25 BA 21 0D 5C 19 22 E7 A1 36 C6 A9 D6
           E1 2F 5D 5E DC E5 E4 D3 D1 2F D9 73 F0 39 71 6B 75 56 D5 61
           76 8A 61 24 E8 1D E5 20 AD 49 BF 36 6B EF 3A F7 B9 B6 0A 50
           6D B0 9B C3 AC 66 4C 8B 60 DA 93 CB 16 70 5A C0 C8 3A CD 14
           D5 16 D0 11 A1 70 30 74 77 FD B5 18 D1 7B 7F FA A4

Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 51 68 FF 90 AF 02 07 75 3C CC D9 65 64 62 A2 12 B8 59 72 3B


Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 36 7E D7 0F 0B 28 B4 5C 33 0E 6 [...]
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the 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 the 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 this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

http://www.nessus.org/u?ae636e78

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

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

Plugin Information

Published: 2016/12/08, Modified: 2021/11/19

Plugin Output

tcp/443/www

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

|-Subject             : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance EV Root
 CA
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Nov 10 00:00:00 2006 GMT
|-Valid To            : Nov 10 00:00:00 2031 GMT
```

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
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-ECDSA-DES-CBC3-SHA      0xC0, 0x08       ECDH          ECDSA    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
    ----------------------        ----------       ---           ----     ---------------------  ---
```

```
    ECDHE-ECDSA-AES128-SHA        0xC0, 0x09       ECDH           ECDSA    AES-CBC(128)
 SHA1
    ECDHE-ECDSA-AES256-SHA        0xC0, 0x0A       ECDH           ECDSA    AES-CBC(256)
 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

The fields above are :

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

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/man1.1.0/apps/ciphers.html

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

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 : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    TLS_AES_128_GCM_SHA256        0x13, 0x01       -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02       -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03       -             -        ChaCha20-Poly1305(256)
 AEAD


SSL Version : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    ECDHE-ECDSA-DES-CBC3-SHA      0xC0, 0x08       ECDH          ECDSA    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
   ----------------------        ----------       ---           ----     --------------------   ---
   ECDHE-ECDSA-AES128-SHA256     0xC0, 0x2B       ECDH          ECDSA    AES-GCM(128)
SHA256
   ECDHE-ECDSA-AES256-SHA384     0xC0, 0x2C       ECDH          ECDSA    AES-GCM(256)
SHA384
   ECDHE-ECDSA-CHACHA20-POLY1305 0xCC, 0xA9       ECDH          ECDSA    ChaCha20-Poly1305(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384
   ECDHE- [...]
```

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
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-ECDSA-DES-CBC3-SHA      0xC0, 0x08       ECDH          ECDSA    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
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-ECDSA-AES128-SHA256     0xC0, 0x2B       ECDH          ECDSA    AES-GCM(128)
 SHA256
```

```
    ECDHE-ECDSA-AES256-SHA384     0xC0, 0x2C       ECDH           ECDSA    AES-GCM(256)
  SHA384
    ECDHE-ECDSA-CHACHA20-POLY1305 0xCC, 0xA9       ECDH           ECDSA    ChaCha20-Poly1305(256)
  SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH           RSA      AES-GCM(128)
  SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH           RSA      AES-GCM(256)
  SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH           RSA      ChaCha20-Poly1305(256)
  SHA256
    ECDHE-ECDSA-AES128-SHA        0xC0, 0x09       ECDH           ECDSA    AES-CBC(128)
  SHA1
    ECDHE-ECDSA-AES256-SHA        0xC0, 0x0A       ECDH           ECDSA    AES-CBC(256)
  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

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/443/www

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

|-Subject             : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance EV Root
 CA
|-Issuer              : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance EV Root
 CA
|-Valid From          : Nov 10 00:00:00 2006 GMT
|-Valid To            : Nov 10 00:00:00 2031 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

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: 2021/04/14

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: 2021/04/14

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.
```

42822 - Strict Transport Security (STS) Detection

Synopsis

The remote web server implements Strict Transport Security.

Description

The remote web server implements Strict Transport Security (STS).

The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.

All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

See Also

http://www.nessus.org/u?2fb3aca6

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/16, Modified: 2019/11/22

Plugin Output

tcp/443/www

```
The STS header line is :

Strict-Transport-Security: max-age=15552000; preload
```

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

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/html/rfc7301

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
http/1.1
h2
```

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.
```

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.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

https://tools.ietf.org/html/rfc8446

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2020/07/09

Plugin Output

tcp/443/www

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

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 192.168.1.10 to 157.240.239.35 :
192.168.1.10
192.168.1.1
117.220.176.1
218.248.175.65
218.248.115.82
?
103.27.168.158
74.119.78.33
157.240.39.81
?
157.240.239.35

Hop Count: 10
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2020/06/12

Plugin Output

tcp/80/www

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 301
rather than 404. The requested URL was :

    http://edge-star-mini-shv-02-del1.facebook.com/XWFU18krrmPc.html
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2020/06/12

Plugin Output

tcp/443/www

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 302
rather than 404. The requested URL was :

    https://edge-star-mini-shv-02-del1.facebook.com/XWFU18krrmPc.html
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/80/www

```
Contents of robots.txt :

# Notice: Collection of data on Facebook through automated means is
# prohibited unless you have express written permission from Facebook
# and may only be conducted for the limited purpose contained in said
# permission.
# See: http://www.facebook.com/apps/site_scraping_tos_terms.php

User-agent: Applebot
Disallow: /ajax/
Disallow: /album.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /dialog/
Disallow: /fbml/ajax/dialog/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /job_application/
Disallow: /l.php
Disallow: /moments_app/
```

```
Disallow: /p.php
Disallow: /photo.php
Disallow: /photos.php
Disallow: /share.php
Disallow: /share/
Disallow: /sharer.php
Disallow: /sharer/
Disallow: /tr/
Disallow: /tr?

User-agent: baiduspider
Disallow: /ajax/
Disallow: /album.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /dialog/
Disallow: /fbml/ajax/dialog/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /job_application/
Disallow: /l.php
Disallow: /moments_app/
Disallow: /p.php
Disallow: /photo.php
Disallow: /photos.php
Disallow: /share.php
Disallow: /share/
Disallow: /sharer.php
Disallow: /sharer/
Disallow: /tr/
Disallow: /tr?

User-agent: Bingbot
Disallow: /ajax/
Disallow: /album.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /dialog/
Disallow: /fbml/ajax/dialog/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /job_application/
Disallow: /l.php
Disallow: /moments_app/
Disallow: /p.php
Disallow: /photo.php
Disallow: /photos.php
Disallow: /share.php
Disallow: /share/
Disallow: /sharer.php
Disallow: /sharer/
Disallow: /tr/
Disallow: /tr?

User-agent: Discordbot
Disallow: /
Disallow: /ajax/
Disallow: /album.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /dialog/
Disallow: /fbml/ajax/dialog/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /job_application/
Disallow: /l.php
Disallow: /moments_app/
Disallow: /p.php
Disallow: /photo.php
Disallow: /photos.php
```

```
Disallow: /share.php
Disallow: /share/
Disallow [...]
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/443/www

```
Contents of robots.txt :

# Notice: Collection of data on Facebook through automated means is
# prohibited unless you have express written permission from Facebook
# and may only be conducted for the limited purpose contained in said
# permission.
# See: http://www.facebook.com/apps/site_scraping_tos_terms.php

User-agent: Applebot
Disallow: /ajax/
Disallow: /album.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /dialog/
Disallow: /fbml/ajax/dialog/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /job_application/
Disallow: /l.php
Disallow: /moments_app/
```

```
Disallow: /p.php
Disallow: /photo.php
Disallow: /photos.php
Disallow: /share.php
Disallow: /share/
Disallow: /sharer.php
Disallow: /sharer/
Disallow: /tr/
Disallow: /tr?

User-agent: baiduspider
Disallow: /ajax/
Disallow: /album.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /dialog/
Disallow: /fbml/ajax/dialog/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /job_application/
Disallow: /l.php
Disallow: /moments_app/
Disallow: /p.php
Disallow: /photo.php
Disallow: /photos.php
Disallow: /share.php
Disallow: /share/
Disallow: /sharer.php
Disallow: /sharer/
Disallow: /tr/
Disallow: /tr?

User-agent: Bingbot
Disallow: /ajax/
Disallow: /album.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /dialog/
Disallow: /fbml/ajax/dialog/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /job_application/
Disallow: /l.php
Disallow: /moments_app/
Disallow: /p.php
Disallow: /photo.php
Disallow: /photos.php
Disallow: /share.php
Disallow: /share/
Disallow: /sharer.php
Disallow: /sharer/
Disallow: /tr/
Disallow: /tr?

User-agent: Discordbot
Disallow: /
Disallow: /ajax/
Disallow: /album.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /dialog/
Disallow: /fbml/ajax/dialog/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /job_application/
Disallow: /l.php
Disallow: /moments_app/
Disallow: /p.php
Disallow: /photo.php
Disallow: /photos.php
```

```
Disallow: /share.php
Disallow: /share/
Disallow [...]
```