My Basic Network Scan

Report generated by Tenable Nessus™ Wed, 13 Nov 2024 15:14:47 EST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.100.157

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	2	0	23

Scan Information

Start time: Wed Nov 13 15:03:12 2024
End time: Wed Nov 13 15:10:43 2024

Host Information

IP: 192.168.100.157
OS: CISCO PIX 7.0

Vulnerabilities

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=portal-service.iem.svc
|-Issuer  : CN=portal-service.iem.svc
```

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=portal-service.iem.svc
```

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: 2024/11/12

Plugin Output

tcp/0

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

  cpe:/o:cisco:pix_firewall:7.0 -> Cisco PIX Firewall Software

Following application CPE matched on the remote system :

  cpe:/a:nginx:nginx -> Nginx
```

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 : firewall
Confidence level : 70
```

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 :

nginx
```

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 is 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: 2024/02/26

Plugin Output

tcp/443/www

```
Response Code : HTTP/1.1 301 Moved Permanently

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: nginx
  Date: Wed, 13 Nov 2024 20:06:48 GMT
  Content-Type: text/html
  Content-Length: 162
  Connection: keep-alive
  Location: https://192.168.100.157/device/edge/
  Cache-Control: no-cache, no-store, must-revalidate
  Pragma: no-cache
  Expires: 0
  Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
  X-XSS-Protection: 1; mode=block
  X-Content-Type-Options: nosniff
  X-Frame-Options: SAMEORIGIN
  Content-Security-Policy: img-src 'self' data:; style-src 'self' 'unsafe-inline'; font-src 'self'
 data:; frame-src 'self';  object-src 'self'; frame-ancestors 'self'

Response Body :
```

```
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

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: 2024/05/20

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: 2024/10/04

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202411131550
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : My Basic Network Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.138.128
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 35.999 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/11/13 15:03 EST
Scan duration : 433 sec
Scan for malware : no
```

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: 2024/10/14

Plugin Output

tcp/0

```
Remote operating system : CISCO PIX 7.0
Confidence level : 70
Method : SinFP


The remote host is running CISCO PIX 7.0
```

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: 2023/07/10

Plugin Output

tcp/443/www

```
This port supports 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/443/www

```
Subject Name:

Common Name: 192.168.100.157

Issuer Name:

Common Name: portal-service.iem.svc

Serial Number: 3F 9D 7A 9D D9 FC 71 1C 9C 26 82 AF 0C FE D0 E1 FE B2 E4 FE

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 13 19:26:28 2024 GMT
Not Valid After: Feb 16 19:26:28 2027 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 B6 93 DE BC 78 71 EC 66 7A 58 50 38 8E 74 FE DB 0E 67 A8
            2F E6 D2 BC 79 9E D9 B2 0A D6 DE 20 38 1E 3B 85 E3 04 D5 88
            B9 B0 E8 21 66 04 9D 39 91 F0 55 00 BE 70 78 99 81 57 52 F6
            A1 22 BB 86 CD 1C 87 25 09 56 63 FD 02 DC FB 3C 36 62 EA BA
            3D A6 2F 1C 0F B7 5F EA 4B EF 3E 2C AF C5 3A 8B 2F 91 53 0A
            93 6F 99 18 36 B1 B1 C2 14 02 59 4A 86 E4 B5 A5 08 DA C1 08
            DF C9 07 0C 77 45 EF 4B 54 C1 C3 53 E8 C9 3C A7 AC 39 C5 40
            9B 7F C3 D7 B9 7E DE 94 27 78 24 BF FA 56 95 FD 1D 68 F7 15
            A5 42 92 1B 24 7D 4A 43 DC 39 48 4E 61 60 D6 11 04 BD 2F 01
            FD 7A E1 41 13 A9 8B 73 70 6A 8F 6D CC 14 E4 6C 30 C8 0A 02
            E5 1E 0D 36 11 E4 A5 D9 14 95 1D 23 87 01 BC 83 DD 6C 81 9A
```

```
8C BC F8 52 9D 3A D5 22 CE E3 CB CD 73 1F 8D 60 FB 76 E0 64
E6 90 A7 88 58 01 4A 6D AC D1 B8 EA C4 B2 F4 78 CE 3D 46 FB
BF 7A 73 D6 1D D1 EE 59 A3 14 E6 25 87 5E 82 13 2D 04 D1 87
48 3B 0A C1 E5 B3 15 00 78 5C 09 82 17 2C 31 B9 E0 4D C3 26
D0 49 B8 65 EE E1 C7 68 D6 26 5B D8 7D B3 CC E0 07 13 C8 19
7C D7 5A D1 0C 7C 24 C6 48 0C 95 72 04 B8 34 F4 79 86 59 3C
82 9F 87 31 2B F4 73 48 D9 88 8E 82 F3 D0 B8 18 AF 46 26 A8
EF 4C FF EE 5E FB A8 0D 05 98 B4 FA FF E9 B3 C4 60 4A C7 C6
06 66 17 97 9D 57 2C 3F C5 80 75 B2 A9 5F BE E1 4A C2 0E E9
95 46 40 AA A0 3C D4 D3 A1 A1 19 7D CA B4 EF E1 27 14 B7 48
74 15 C2 CE 50 34 8E 55 80 6A EF C0 05 4A A6 73 20 8D E6 C9
87 1B 6E CF B8 3C E3 68 B8 96 E4 D5 59 EF [...]
```

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 :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ----------------------  ---
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDH          RSA      AES-CBC(256)
 SHA384

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/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

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
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDH          RSA      AES-CBC(256)
 SHA384

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 :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDH          RSA      AES-CBC(256)
 SHA384

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             : CN=portal-service.iem.svc
|-Issuer              : CN=portal-service.iem.svc
|-Valid From          : Nov 13 19:10:44 2024 GMT
|-Valid To            : Oct 20 19:10:44 2124 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
```

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 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_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

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: 2024/02/12

Plugin Output

tcp/443/www

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


  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     --------------------    ---
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDH          RSA      AES-CBC(256)
 SHA384

The fields above are :

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

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: 2024/03/26

Plugin Output

tcp/443/www

```
A TLSv1.2 server answered on this port.
```

tcp/443/www

```
A web server is running on this port through TLSv1.2.
```

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=63072000; includeSubDomains; preload
```

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: 2024/09/11

Plugin Output

tcp/443/www

```
http/1.1
```

87242 - TLS NPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS NPN extension.

Description

The remote host supports the TLS NPN (Transport Layer Security Next Protocol Negotiation) extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/id/draft-agl-tls-nextprotoneg-03.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/12/08, Modified: 2024/09/11

Plugin Output

tcp/443/www

```
NPN Supported Protocols:

  http/1.1
```

62564 - TLS Next Protocols Supported

Synopsis

The remote service advertises one or more protocols as being supported over TLS.

Description

This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections.

Note that Nessus did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and / or failing to advertise other supported protocols.

See Also

https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

https://technotes.googlecode.com/git/nextprotoneg.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/10/16, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
The target advertises that the following protocols are
supported over SSL / TLS:

  http/1.1
```

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.
```

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: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.138.128 to 192.168.100.157 :
192.168.138.128
192.168.138.2
?
192.168.100.157

Hop Count: 4
```

106375 - nginx HTTP Server Detection

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

https://nginx.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0677

Plugin Information

Published: 2018/01/26, Modified: 2023/05/24

Plugin Output

tcp/443/www

```
URL     : https://192.168.100.157/
Version : unknown
source  : Server: nginx
```

192.168.100.179

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	4	0	45

Scan Information

Start time: Wed Nov 13 15:03:12 2024
End time: Wed Nov 13 15:14:44 2024

Host Information

IP: 192.168.100.179
OS: CISCO PIX 7.0

Vulnerabilities

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 : C=Edge/ST=/L=/2.5.4.9=/O=/OU=/CN=Industiral
|-Issuer  : C=Edge/ST=/L=/2.5.4.9=/O=/OU=/CN=Industiral
```

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/4443/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 : C=Edge/ST=/L=/2.5.4.9=/O=/OU=/CN=Industiral
|-Issuer  : C=Edge/ST=/L=/2.5.4.9=/O=/OU=/CN=Industiral
```

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 : C=Edge/ST=/L=/2.5.4.9=/O=/OU=/CN=Industiral
```

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/4443/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 : C=Edge/ST=/L=/2.5.4.9=/O=/OU=/CN=Industiral
```

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: 2024/11/12

Plugin Output

tcp/0

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

  cpe:/o:cisco:pix_firewall:7.0 -> Cisco PIX Firewall Software

Following application CPE matched on the remote system :

  cpe:/a:nginx:nginx -> Nginx
```

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 : firewall
Confidence level : 70
```

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 :

nginx
```

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/4443/www

```
The remote web server type is :

nginx
```

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 is 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: 2024/02/26

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 301 Moved Permanently

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: nginx
  Date: Wed, 13 Nov 2024 20:07:11 GMT
  Content-Type: text/html
  Content-Length: 162
  Connection: keep-alive
  Location: https://192.168.100.179:4443/

Response Body :

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</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 is 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: 2024/02/26

Plugin Output

tcp/443/www

```
Response Code : HTTP/1.1 302 Moved Temporarily

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Date: Wed, 13 Nov 2024 20:07:11 GMT
  Content-Type: text/html
  Content-Length: 110
  Connection: keep-alive
  x-frame-options: SAMEORIGIN
  X-XSS-Protection: 0
  X-Content-Type-Options: nosniff
  Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
  Referrer-Policy: strict-origin
  Set-Cookie: session=mfFBuQBrdsD2zarM9N1KIg|1731532031|37Kt-
huW8CGfi6P8gdBkwho0XdeE3_cB2HVy8U1DlSpgUbD_BS-
G8PQU5C6KXE_5muvAO3_9PJEgZS9Dw2H27BmaftNS1j6y6plOpxQY6UVmWKQ6lPR9JsSmDDpT8T7dhEzXLGB89DasfMfUfNLGHjjXAyqMeHhhgI3v8
8LaHxahzFmEWEwVKfzFbMWg_kkE; Path=/; SameSite=Lax; Secure; HttpOnly
  Cache-Control: no-cache, no-store, max-age=0
  Location: https://192.168.100.179/auth/realms/customer/protocol/openid-
connect/auth?nonce=6bd02b885ccabc610de606a42d951164&redirect_uri=https%3A%2F
```

```
%2F192.168.100.179%2Fcb&response_type=code&state=9006f0a9557306c7754e8a1ee6e81c8b&client_id=ie-
management&scope=openid

Response Body :

<html>
<head><title>302 Found</title></head>
<body>
<center><h1>302 Found</h1></center>
</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 is 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: 2024/02/26

Plugin Output

tcp/4443/www

```
Response Code : HTTP/1.1 301 Moved Permanently

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: nginx
  Date: Wed, 13 Nov 2024 20:07:11 GMT
  Content-Type: text/html
  Content-Length: 162
  Connection: keep-alive
  Location: https://192.168.100.179:4443/webui/
  X-Frame-Options: SAMEORIGIN
  X-Content-Type-Options: nosniff
  Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
  X-XSS-Protection: 1; mode=block
  Content-Security-Policy: img-src 'self' data:; style-src 'self' 'unsafe-inline'; font-src 'self'
 data:; frame-src 'self';  object-src 'self'; frame-ancestors 'self'
  Cache-Control: no-cache, no-store, must-revalidate
  Pragma: no-cache
  Expires: 0

Response Body :
```

```
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

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: 2024/05/20

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: 2024/05/20

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: 2024/05/20

Plugin Output

tcp/4443/www

```
Port 4443/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: 2024/10/04

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202411131550
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : My Basic Network Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.138.128
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 53.476 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/11/13 15:03 EST
Scan duration : 682 sec
Scan for malware : no
```

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: 2024/10/14

Plugin Output

tcp/0

```
Remote operating system : CISCO PIX 7.0
Confidence level : 70
Method : SinFP


The remote host is running CISCO PIX 7.0
```

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: 2023/07/10

Plugin Output

tcp/443/www

```
This port supports TLSv1.3/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: 2023/07/10

Plugin Output

tcp/4443/www

```
This port supports 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/443/www

```
Subject Name:

Country: Edge
State/Province:
Locality:
Street:
Organization:
Organization Unit:
Common Name: 192.168.100.179

Issuer Name:

Country: Edge
State/Province:
Locality:
Street:
Organization:
Organization Unit:
Common Name: Industiral Intermediate Certificate

Serial Number: 48 82 73 93

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 13 19:08:06 2024 GMT
Not Valid After: Nov 13 19:08:06 2034 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 4096 bits
Public Key: 00 C8 04 0D 09 F5 F7 23 77 25 56 E1 84 A3 0E F4 82 AF 8D AF
            89 A9 3B FA AC B7 9F CC FA 96 7D 39 AF B5 E8 57 0F FF B0 CF
            E2 F3 42 99 ED EC BC B6 32 05 25 9D 20 D0 E8 1F 08 B0 90 7C
            1D 2D 21 E4 5F C3 D2 D1 D8 8D 4B 19 24 D6 52 D5 0D 65 E8 73
            5C 0D 09 81 83 C1 36 A0 9D 76 E5 56 BD 3C 11 AC 15 06 E1 25
            E1 3C 3C 57 F4 AB DD 3E 0C F7 87 9F E4 6D 53 1D B4 26 65 ED
            A4 9C F1 55 35 04 BE 92 7D 44 96 E8 1D E2 06 70 BA 0E DA 76
            2F CE 76 8C D3 99 57 06 A3 7E 39 46 8F D6 46 C5 3F 12 AF 14
            A1 41 F5 85 1E 94 29 73 EC EC 30 9D B4 CC FB 73 18 F2 A3 8F
            F5 33 41 D1 DD 3F E8 AD 6A DC 44 39 FE C1 F2 B5 6B DE C9 EE
            16 F8 42 B7 72 20 5A 31 55 7D 63 18 10 4C AB 9B 37 55 DB 74
            24 50 E3 7D 95 68 12 85 BE D4 84 AF 5B CC 6A 4F 72 1B B6 31
            DE C7 C2 6F 4B 6F 2F 4C 67 DE E1 8E 9E D9 E7 B1 81 DF 30 8E
            7C 4D D9 52 01 69 D6 A6 05 98 09 F4 46 A3 7B 46 62 6A DA 95
            CD 94 E5 BE 3A 19 5D BC 87 3F 7E 70 06 0D C3 5E F5 58 1A 26
            8F AA 97 66 01 C8 46 A2 27 8E B9 87 4D 2D 44 16 BE F2 FA 74
            FD 6F 9A 28 9D 03 20 9F 77 BB 0F 68 93 CD 0A 62 CD D1 02 C1
            00 1A A6 3A 2A B0 03 1C FB 7C 44 C6 14 80 48 0D 5E 6C 03 6E
            B7 CA 67 04 68 06 32 EF FD C9 89 CC 07 AB AE 19 DC 5F 6E 5D
            66 31 15 DD 34 EA 1D 67 14 5C 58 33 98 05 54 4F EE 47 FD DA
            37 EB 50 08 E2 5F 2C 2A FC 8D E9 10 29 C6 B0 7D F9 [...]
```

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/4443/www

```
Subject Name:

Country: Edge
State/Province:
Locality:
Street:
Organization:
Organization Unit:
Common Name: 192.168.100.179

Issuer Name:

Country: Edge
State/Province:
Locality:
Street:
Organization:
Organization Unit:
Common Name: Industiral Intermediate Certificate

Serial Number: 48 82 73 93

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 13 19:08:06 2024 GMT
Not Valid After: Nov 13 19:08:06 2034 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 4096 bits
Public Key: 00 C8 04 0D 09 F5 F7 23 77 25 56 E1 84 A3 0E F4 82 AF 8D AF
            89 A9 3B FA AC B7 9F CC FA 96 7D 39 AF B5 E8 57 0F FF B0 CF
            E2 F3 42 99 ED EC BC B6 32 05 25 9D 20 D0 E8 1F 08 B0 90 7C
            1D 2D 21 E4 5F C3 D2 D1 D8 8D 4B 19 24 D6 52 D5 0D 65 E8 73
            5C 0D 09 81 83 C1 36 A0 9D 76 E5 56 BD 3C 11 AC 15 06 E1 25
            E1 3C 3C 57 F4 AB DD 3E 0C F7 87 9F E4 6D 53 1D B4 26 65 ED
            A4 9C F1 55 35 04 BE 92 7D 44 96 E8 1D E2 06 70 BA 0E DA 76
            2F CE 76 8C D3 99 57 06 A3 7E 39 46 8F D6 46 C5 3F 12 AF 14
            A1 41 F5 85 1E 94 29 73 EC EC 30 9D B4 CC FB 73 18 F2 A3 8F
            F5 33 41 D1 DD 3F E8 AD 6A DC 44 39 FE C1 F2 B5 6B DE C9 EE
            16 F8 42 B7 72 20 5A 31 55 7D 63 18 10 4C AB 9B 37 55 DB 74
            24 50 E3 7D 95 68 12 85 BE D4 84 AF 5B CC 6A 4F 72 1B B6 31
            DE C7 C2 6F 4B 6F 2F 4C 67 DE E1 8E 9E D9 E7 B1 81 DF 30 8E
            7C 4D D9 52 01 69 D6 A6 05 98 09 F4 46 A3 7B 46 62 6A DA 95
            CD 94 E5 BE 3A 19 5D BC 87 3F 7E 70 06 0D C3 5E F5 58 1A 26
            8F AA 97 66 01 C8 46 A2 27 8E B9 87 4D 2D 44 16 BE F2 FA 74
            FD 6F 9A 28 9D 03 20 9F 77 BB 0F 68 93 CD 0A 62 CD D1 02 C1
            00 1A A6 3A 2A B0 03 1C FB 7C 44 C6 14 80 48 0D 5E 6C 03 6E
            B7 CA 67 04 68 06 32 EF FD C9 89 CC 07 AB AE 19 DC 5F 6E 5D
            66 31 15 DD 34 EA 1D 67 14 5C 58 33 98 05 54 4F EE 47 FD DA
            37 EB 50 08 E2 5F 2C 2A FC 8D E9 10 29 C6 B0 7D F9 [...]
```

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/4443/www

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ----------------------  ---
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDH          RSA      AES-CBC(256)
 SHA384

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/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

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
  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-CHACHA20-POLY1305     0xCC, 0xAA       DH            RSA      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

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/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/4443/www

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

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDH          RSA      AES-CBC(256)
 SHA384

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 :

  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-CHACHA20-POLY1305     0xCC, 0xAA        DH            RSA      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

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/4443/www

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDH          RSA      AES-CBC(256)
 SHA384

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=Edge/ST=/L=/2.5.4.9=/O=/OU=/CN=Industiral
|-Issuer              : C=Edge/ST=/L=/2.5.4.9=/O=/OU=/CN=Industiral
|-Valid From          : Nov 13 19:08:05 2024 GMT
|-Valid To            : Nov 13 19:08:05 2034 GMT
|-Signature Algorithm : SHA-256 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/4443/www

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

|-Subject             : C=Edge/ST=/L=/2.5.4.9=/O=/OU=/CN=Industiral
|-Issuer              : C=Edge/ST=/L=/2.5.4.9=/O=/OU=/CN=Industiral
|-Valid From          : Nov 13 19:08:05 2024 GMT
|-Valid To            : Nov 13 19:08:05 2034 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
```

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 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_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

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: 2024/02/12

Plugin Output

tcp/443/www

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


  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

The fields above are :

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

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 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_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

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: 2024/02/12

Plugin Output

tcp/4443/www

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


  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     --------------------    ---
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDH          RSA      AES-CBC(256)
 SHA384

The fields above are :

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

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: 2024/03/26

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: 2024/03/26

Plugin Output

tcp/443/www

```
A TLSv1.2 server answered on this port.
```

tcp/443/www

```
A web server is running on this port through TLSv1.2.
```

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: 2024/03/26

Plugin Output

tcp/4443/www

```
A TLSv1.2 server answered on this port.
```

tcp/4443/www

```
A web server is running on this port through TLSv1.2.
```

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=63072000; includeSubDomains; preload
```

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/4443/www

```
The STS header line is :

Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
```

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: 2024/09/11

Plugin Output

tcp/443/www

```
http/1.1
```

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: 2024/09/11

Plugin Output

tcp/4443/www

```
http/1.1
```

87242 - TLS NPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS NPN extension.

Description

The remote host supports the TLS NPN (Transport Layer Security Next Protocol Negotiation) extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/id/draft-agl-tls-nextprotoneg-03.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/12/08, Modified: 2024/09/11

Plugin Output

tcp/4443/www

```
NPN Supported Protocols:

  http/1.1
```

62564 - TLS Next Protocols Supported

Synopsis

The remote service advertises one or more protocols as being supported over TLS.

Description

This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections.

Note that Nessus did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and / or failing to advertise other supported protocols.

See Also

https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

https://technotes.googlecode.com/git/nextprotoneg.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/10/16, Modified: 2022/04/11

Plugin Output

tcp/4443/www

```
The target advertises that the following protocols are
supported over SSL / TLS:

  http/1.1
```

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/4443/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: 2023/12/13

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: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.138.128 to 192.168.100.179 :
192.168.138.128
192.168.138.2
192.168.100.179

Hop Count: 2
```

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: 2022/06/17

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://192.168.100.179/rZQJ93EIWOlK.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: 2022/06/17

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://192.168.100.179/rZQJ93EIWOlK.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: 2022/06/17

Plugin Output

tcp/4443/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 :

    https://192.168.100.179:4443/rZQJ93EIWOlK.html
```

106375 - nginx HTTP Server Detection

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

https://nginx.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0677

Plugin Information

Published: 2018/01/26, Modified: 2023/05/24

Plugin Output

tcp/80/www

```
URL     : http://192.168.100.179/
Version : unknown
source  : Server: nginx
```

106375 - nginx HTTP Server Detection

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

https://nginx.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0677

Plugin Information

Published: 2018/01/26, Modified: 2023/05/24

Plugin Output

tcp/4443/www

```
URL     : https://192.168.100.179:4443/
Version : unknown
source  : Server: nginx
```