My Basic Network Scan

Report generated by Tenable Nessus™ Fri, 08 Aug 2025 18:28:54 BST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

212.82.100.137

0	0	2	0	32
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

DNS Name:	ats1.l7.search.vip.ir2.yahoo.com
IP:	212.82.100.137
OS:	CISCO PIX 7.0

Vulnerabilities

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)

References

XREF	CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

tcp/443/www

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

157288 - TLS Version 1.1 Deprecated Protocol

Synopsis

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

Description

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

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

See Also

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

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/443/www

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

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: 2025/07/14

Plugin Output

tcp/0

```

The remote operating system matched the following CPE :

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

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: 2025/03/12

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 :

ATS
```

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: 2025/03/13

Plugin Output

tcp/0

```
212.82.100.137 resolves as ats1.l7.search.vip.ir2.yahoo.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 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/1.1 500 INKApi Error

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

  Date: Fri, 08 Aug 2025 17:09:07 GMT
  Connection: close
  Server: ATS
  X-Content-Type-Options: nosniff
  X-XSS-Protection: 1; mode=block; report=https://csp.search.yahoo.com/xssreport
  Referrer-Policy: no-referrer-when-downgrade
  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: 2025/07/14

Plugin Output

tcp/21

```
Port 21/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/80

```
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: 2025/07/14

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: 2025/07/14

Plugin Output

tcp/1723

```
Port 1723/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: 2025/06/25

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.9.2
Nessus build : 20017
Plugin feed version : 202508080803
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 : 192.168.130.129
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 215.951 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 : yes
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 : 2025/8/8 17:55 BST (UTC +01:00)
Scan duration : 1304 sec
Scan for malware : no
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, “OS Identification”, the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Juniper ScreenOS
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : CISCO PIX 7.0
Confidence level : 70
Method : SinFP
Type : firewall
Fingerprint : SinFP:
   P1:B11013:F0x12:W64240:O0204ffff:M1460:
   P2:B11013:F0x12:W64240:O0204ffff:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:191302_7_p=80R

Following fingerprints could not be used to determine OS :
 HTTP:!:server: ATS

SSLcert:!:i/CN:DigiCert SHA2 High Assurance Server CAi/O:DigiCert Inci/OU:www.digicert.coms/
CN:*.answers.search.yahoo.coms/O:Yahoo Holdings Inc.
d1ca5fc6916d92a11445fdf1405f185f8d3ae12f
```

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: 2025/06/03

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
```

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: 2025/06/16

Plugin Output

tcp/443/www

```
This port supports TLSv1.3/TLSv1.0/TLSv1.1/TLSv1.2.
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

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

Description

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

```

The host name known by Nessus is :

  ats1.17.search.vip.ir2.yahoo.com

The Common Name in the certificate is :

  *.answers.search.yahoo.com

The Subject Alternate Names in the certificate are :

  *.answers.search.yahoo.com
  *.autos.search.yahoo.com
  *.blog.search.yahoo.com
  *.celebrity.search.yahoo.com
  *.dictionary.search.yahoo.com
  *.finance.search.yahoo.com
  *.forum.search.yahoo.com
  *.games.search.yahoo.com
  *.images.search.yahoo.com
  *.knowledge.search.yahoo.com
  *.lifestyle.search.yahoo.com
  *.local.search.yahoo.com
  *.local.yahoo.com
  *.maps.yahoo.com
  *.movies.search.yahoo.com
  *.news.search.yahoo.com
  *.recherche.aol.fr
  *.recipes.search.yahoo.com
```

```
    *.search.aol.ca
    *.search.aol.co.uk
    *.search.aol.com
    *.search.engadget.com
    *.search.techcrunch.com
    *.search.yahoo.com
    *.search.yahoo.net
    *.shine.search.yahoo.com
    *.shopping.search.yahoo.com
    *.solo-search.com
    *.sports.search.yahoo.com
    *.suche.aol.de
    *.tv.search.yahoo.com
    *.video.search.yahoo.com
    *.yhs4.search.yahoo.com
    *.ysm.yahoo.com
    answers.yahoo.com
    api-partnerinsights.yahoo.com
    baltimoresun.search.yahoo.com
    boss.yahoo.com
    chat.yahoo.com
    chicagotribune.search.yahoo.com
    courant.search.yahoo.com
    dailypress.search.yahoo.com
    downloads.yahoo.com
    hk.dictionary.yahoo.com
    local.yahoo.com
    maps.yahoo.com
    mcall.search.yahoo.com
    msapp.yahooapis.com
    nydailynews.searchboss.com
    orlandosentinel.search.yahoo.com
    partnerinsights.yahoo.com
    pilotonline.search.yahoo.com
    recherche.aol.fr
    reseller.yahoo.com
    search.aol.ca
    search.aol.co.uk
    search.aol.com
    search.cashay.com
    search.engadget.com
    search.intheknow.com
    search.techcrunch.com
    search.yahoo.com
    search.yahoo.net
    solo-search.com
    suche.aol.de
    sun-sentinel.search.yahoo.com
    tw.dictionary.yahoo.com
    yboss.yahooapis.com
    ysp.yahooapis.com
```

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: New York
Locality: New York
Organization: Yahoo Holdings Inc.
Common Name: *.answers.search.yahoo.com

Issuer Name:

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

Serial Number: 0D 9F 26 40 A0 92 A8 97 36 95 B4 CD 04 B8 2F 08

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Apr 15 00:00:00 2025 GMT
Not Valid After: Oct 08 23:59:59 2025 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 50 8A 51 6A 7E FB AF 39 2C 18 DA 56 1B 8D 61 6B 5E 7F 11 0D
              B2 06 CF 92 FE 9B 27 25 E8 D2 85 43
Public Key Y: 86 79 09 30 01 D5 07 9D E7 F5 EC 91 00 FD 91 06 C8 9B 33 36
```

```
              F1 A1 01 EC B0 81 96 A4 7C 7C F3 D9

Signature Length: 256 bytes / 2048 bits
Signature: 00 44 0A 65 77 AD 68 ED 4E 86 B5 86 37 13 7B EE 40 08 51 32
           12 E3 95 3D CA E1 66 8F 08 C5 32 35 68 7C 50 A6 FF C6 31 5F
           34 11 95 58 11 89 75 20 11 13 94 04 E2 9F E1 CE CE 33 38 DD
           CD AD B4 73 94 86 8B 0A FD FF 6E B8 68 DA C9 AC 7A C9 C9 DB
           E7 80 22 41 DC 37 0A 90 2F 2D 9A 26 E5 80 8E E6 55 26 F3 A0
           A3 F5 5D 43 26 5B E1 0D 4C 9C FF E8 D8 31 39 DC F3 8E B8 EC
           14 D8 A0 C4 B0 D6 44 B6 54 46 F9 91 6B E8 F5 CF 6E 45 B3 A3
           A8 D9 F7 28 57 80 42 E7 40 74 39 72 62 7F C4 68 E9 7E 6D 54
           39 6F E1 27 AF 82 5A 91 26 D0 53 8A EF 38 91 D2 99 9C 05 3C
           9F B3 D1 E5 C3 87 E8 73 39 9E 2E 6F 3C 78 D0 31 24 E4 01 9D
           FE BD 5E 82 F3 07 93 EC 0E A9 C2 52 00 CC 87 07 D1 13 E2 8D
           A1 60 ED D8 A0 09 14 C2 B6 E1 14 7E 1D A3 47 36 95 C4 43 11
           C6 32 5D D7 5A EC 41 5B CB F6 16 B3 2E C6 41 E0 48

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: 44 D1 F3 E4 28 0C 5D [...]
```

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 (CVE-2004-2761, for example). 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
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

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
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIDxTCCAq2gAwIBAgIQAqxcJmoLQJuPC3nyrkYldzANBgkqhkiG9w0BAQUFADBsMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMR
+9S75S0tMqbf5YE/
yc0lSbZxKsPVlDRnogocsF9ppkCxxLeyj9CYpKlBWTrT3JTWPNt0OKRKzE0lgvdKpVMSOO7zSW1xkX5jtqumX8OkhPhPYlG+
+MXs2ziS4wblCJEMxChBVfvLWokVfnHoNb9Ncgk9vjo4UFt3MRuNs8ckRZqnrG0AFFoEt7oT61EKmEFBIk5lYYeBQVCmeVyJ3hlKV9Uu5l0cUyx
+mM0aBhakaHPQNAQTXKFx01p8VdteZOE3hzBWBOURtCmAEvF5OYiiAhF8J2a3iLd48soKqDirCmTCv2ZdlYTBoSUeh10aUAsgEsxBu24LUTi4S8sCA
BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFLE+w2kD+L9HAdSYJhoIAu9jZCvDMB8GA1UdIwQYMBaAFLE+w2kD
+L9HAdSYJhoIAu9jZCvDMA0GCSqGSIb3DQEBBQUAA4IBAQAcGgaX3NecnzyIZgYIVyHbIUf4KmeqvxgydkAQV8GK83rZEWWONfqe/
EW1ntlMMUu4kehDLI6zeM7b41N5cdblIZQB2lWHmiRk9opmzN6cN82oNLFpmyPInngiK3BD41VHMWEZ71jFhS9OMPagMRYjyOfiZRYzy78aG6A9+Mp
S6cCZdkGCevEsXCS+0yx5DaMkHJ8HSXPfqIbloEpw8nL+e/IBcm2PN7EeqJSdnoDfzAIJ9VNep+OkuE6N36B9K
-----END CERTIFICATE-----
```

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-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
     ECDHE-ECDSA-AES128-SHA256     0xC0, 0x23       ECDH          ECDSA    AES-CBC(128)
  SHA256
     ECDHE-ECDSA-AES256-SHA384     0xC0, 0x24       ECDH          ECDSA    AES-CBC(256)
  SHA384
     ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
  SHA256
     ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
  SHA384
     RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
  SHA256
     RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
  SHA256

 The fields above are :

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

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
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-ECDSA-AES-128-CCM-AEAD  0xC0, 0xAC       ECDH          ECDSA    AES-CCM(128)
 AEAD
```

```
   ECDHE-ECDSA-AES-128-CCM8-AEAD 0xC0, 0xAE       ECDH          ECDSA    AES-CCM8(128)
AEAD
   ECDHE-ECDSA-AES128-SHA256     0xC0, 0x2B       ECDH          ECDSA    AES-GCM(128)
SHA256
   ECDHE-ECDSA-AES-256-CCM-AEAD  0xC0, 0xAD       ECDH          ECDSA    AES-CCM(256)
AEAD
   ECDHE-ECDSA-AES-256-CCM8-AEAD 0xC0, 0xAF       ECDH          ECDSA    AES-CCM8(256)
AEAD
   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
   RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA           RSA     [...]
```

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-ECDSA-AES-128-CCM-AEAD  0xC0, 0xAC       ECDH          ECDSA    AES-CCM(128)
 AEAD
    ECDHE-ECDSA-AES-128-CCM8-AEAD 0xC0, 0xAE       ECDH          ECDSA    AES-CCM8(128)
 AEAD
    ECDHE-ECDSA-AES128-SHA256     0xC0, 0x2B       ECDH          ECDSA    AES-GCM(128)
 SHA256
    ECDHE-ECDSA-AES-256-CCM-AEAD  0xC0, 0xAD       ECDH          ECDSA    AES-CCM(256)
 AEAD
    ECDHE-ECDSA-AES-256-CCM8-AEAD 0xC0, 0xAF       ECDH          ECDSA    AES-CCM8(256)
 AEAD
```

```
   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
   ECDHE-ECDSA-AES128-SHA256     0xC0, 0x23       ECDH          ECDSA    AES-CBC(128)
SHA256
   ECDHE-ECDSA-AES256-SHA384     0xC0, 0x24       ECDH          ECDSA    AES-CBC(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128) [...]
```

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
```

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-ECDSA-AES-128-CCM-AEAD  0xC0, 0xAC       ECDH          ECDSA    AES-CCM(128)
 AEAD
    ECDHE-ECDSA-AES-128-CCM8-AEAD 0xC0, 0xAE       ECDH          ECDSA    AES-CCM8(128)
 AEAD
    ECDHE-ECDSA-AES-256-CCM-AEAD  0xC0, 0xAD       ECDH          ECDSA    AES-CCM(256)
 AEAD
    ECDHE-ECDSA-AES-256-CCM8-AEAD 0xC0, 0xAF       ECDH          ECDSA    AES-CCM8(256)
 AEAD
    RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA           RSA      AES-CCM(128)
 AEAD
    RSA-AES-128-CCM8-AEAD         0xC0, 0xA0       RSA           RSA      AES-CCM8(128)
 AEAD
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES-256-CCM-AEAD          0xC0, 0x9D       RSA           RSA      AES-CCM(256)
 AEAD
    RSA-AES-256-CCM8-AEAD         0xC0, 0xA1       RSA           RSA      AES-CCM8(256)
 AEAD
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
    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
    ECDHE-ECDSA-AES128-SHA256     0xC0, 0x23       ECDH       [...]
```

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 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=31536000
```

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
h2
```

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:

  h2
  http/1.1
  http/1.0
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

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

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

See Also

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

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

Solution

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

Risk Factor

None

References

XREF	CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

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: 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 192.168.130.129 to 212.82.100.137 :
192.168.130.129
192.168.130.2
212.82.100.137

Hop Count: 2
```

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 :

User-agent: *
Disallow: /search
Disallow: /bin
Disallow: /language
Disallow: /yhs
Disallow: /aol
Disallow: /reviews
Disallow: /click
Disallow: /local

User-agent: ADmantX
Disallow: /

User-agent: AlphaBot
Disallow: /

User-agent: anthropic-ai
Disallow: /
```

```
User-agent: AwarioRssBot
Disallow: /

User-agent: AwarioSmartBot
Disallow: /

User-agent: BLEXBot
Disallow: /

User-agent: Buzzbot
Disallow: /

User-agent: Bytespider
Disallow: /

User-agent: CCBot
Disallow: /

User-agent: ChatGPT-User
Disallow: /

User-agent: claritybot
Disallow: /

User-agent: Claude-Web
Disallow: /

User-agent: ClaudeBot
Disallow: /

User-agent: cohere-ai
Disallow: /

User-agent: Diffbot
Disallow: /

User-agent: FacebookBot
Disallow: /

User-agent: FriendlyCrawler
Disallow: /

User-agent: Google-Extended
Disallow: /

User-agent: GPTBot
Disallow: /

User-agent: huggingface
Disallow: /

User-agent: ImagesiftBot
Disallow: /

User-agent: img2dataset
Disallow: /

User-agent: magpie-crawler
Disallow: /

User-agent: Meltwater
Disallow: /

User-agent: Neevabot
Disallow: /

User-agent: news-please
Disallow: /
```

```
User-agent: NewsNow
Disallow: /

User-agent: Nutch
Disallow: /

User-agent: omgili
Disallow: /

User-agent: omgilibot
Disallow: /

User-agent: http://panscient.com
Disallow: /

User-agent: Perplexity-ai
Disallow: /

User-agent: PerplexityBot
Disallow: /

User-agent: PetalBot
Disallow: /

User-agent: PiplBot
Disallow: /

User-agent: http://scoop.it
Disallow: /

User-agent: Scrapy
Disallow: /

User-agent: Seekr
Disallow: /

User-agent: SentiBot
Disallow: /

User-agent: SeznamBot
Disallow: /

User-agent: TurnitinBot
Disallow: /

User-agent: YouBot
Disallow: /

User-agent: ZumBot
Disallow: /
```