



mainscan(t4)

Report generated by Nessus™

Sun, 22 Oct 2023 13:03:25 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 9animes.ph.....4

Nessus Essentials

Vulnerabilities by Host

9animes.ph



Scan Information

Start time: Sun Oct 22 12:30:31 2023

End time: Sun Oct 22 13:03:25 2023

Host Information

DNS Name: 9animes.ph

IP: 104.21.28.211

OS: CentOS Linux 7 Linux Kernel 3.10

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

```
TLShv1 is enabled and the server supports at least one cipher.
```

157288 - TLS Version 1.1 Protocol Deprecated

Synopsis

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

Description

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

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

See Also

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

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2023/04/19

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: 2023/10/16

Plugin Output

tcp/0

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

```
cpe:/o:centos:centos -> CentOS
```


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 : unknown  
Confidence level : 56
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

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 :  
cloudflare
```

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 :  
cloudflare
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/8080/www

```
The remote web server type is :  
cloudflare
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

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

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

    Date: Sun, 22 Oct 2023 07:17:48 GMT
    Transfer-Encoding: chunked
    Connection: keep-alive
    Cache-Control: max-age=3600
    Expires: Sun, 22 Oct 2023 08:17:48 GMT
    Location: https://9animes.ph/
    Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report
/v3?s=uY18plL%2FZTgmul4caUnWMidjzld8EZfRn2CIWruzYS2Ira5qH9raK%2BxB
%2FWFa9Frkvx7RxwmIfoiTuOParpXXcsRN9KlVWSmuoZ41bznAQQHY3l9L4dcKlKnpqrq"}],"group":"cf-
nel","max_age":604800}
    NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
    Server: cloudflare
    CF-RAY: 819ff6736fc4036e-FRA
    alt-svc: h3=":443"; ma=86400

Response Body :
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1

SSL : yes

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Date: Sun, 22 Oct 2023 07:17:54 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

vary: Accept-Encoding

link: <https://9animes.ph/wp-json/>; rel="https://api.w.org/"

x-xss-protection: 1; mode=block

x-content-type-options: nosniff

CF-Cache-Status: DYNAMIC

Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=yviAsLD%2FQSu2QK1yieXRA2%2Bze4e4Yny0gbLAX1Q%2Bc96RGVK6b%2B2ghqGJCpbDj9UHG1e4S0%2BgZtDjW00C8vA4sMvcYe%2FFRpZCOKtp%2FCTRhvMsna2zpiVxDLj1D6Ha"}],"group":"cf-nel","max_age":604800}

NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}

Server: cloudflare

CF-RAY: 819ff694df6b3ff3-SIN

alt-svc: h3=":443"; ma=86400

Response Body :

```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "https://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
<html xmlns="https://www.w3.org/1999/xhtml" lang="en-US">
<head profile="http://gmpg.org/xfn/11">
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta name="viewport" content="width=device-width" />
<meta name="theme-color" content="#7f23db">
<meta name="msapplication-navbutton-color" content="#7f23db">
<meta name="apple-mobile-web-app-status-bar-style" content="#7f23db">
<meta name="robots" content="index, follow, max-image-preview:large, max-snippet:-1, max-video-
preview:-1" />

<title>9anime - Watch anime online with English Subtitles</title>
<meta name="description" content="9anime is an anime streaming site where you can watch anime online
with English subtitles. Also download 9 anime videos for free in high quality." />
<link rel="canonical" href="https://9animes.ph/" />
<link rel="next" href="https://9animes.ph/page/2" />
<meta property="og:locale" content="en_US" />
<meta property="og:type" content="website" />
<meta property="og:title" content="9anime - Watch anime online with English Subtitles" />
[...]
```


24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8080/www

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

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

    Date: Sun, 22 Oct 2023 07:17:46 GMT
    Transfer-Encoding: chunked
    Connection: keep-alive
    Cache-Control: max-age=3600
    Expires: Sun, 22 Oct 2023 08:17:46 GMT
    Location: https://9animes.ph/
    Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=E80VZ4V4mu8nARqFtFd7HOM%2BIj%2FJFPfmOPgjN0SWBHgR6RmvrI1epsMCzlnxb45p4ttauv9mSY239DFa4pIyt%2BQlqeeGVxYepdUCDM2CdHwMpr6kSzlCpEBs%2FF7lPxtbfvg%3D"}],"group":"cf-nel","max_age":604800}
    NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
    Server: cloudflare
    CF-RAY: 819ff667d9345fe5-SIN
    alt-svc: h3=":443"; ma=86400

Response Body :
```

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: 2023/09/25

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

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: 2023/09/25

Plugin Output

tcp/443/www

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

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: 2023/09/25

Plugin Output

tcp/8080/www

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

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: 2023/07/31

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.6.1
Nessus build : 20021
Plugin feed version : 202310212203
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : mainscan(t4)
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.5.119
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 339.755 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/10/22 12:30 India Standard Time
Scan duration : 1962 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: 2022/03/09

Plugin Output

tcp/0

```
Remote operating system : CentOS Linux 7 Linux Kernel 3.10
Confidence level : 56
Method : MLSinFP
```

```
The remote host is running CentOS Linux 7 Linux Kernel 3.10
```

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


10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
Subject Name:
Country: US
State/Province: California
Locality: San Francisco
Organization: Cloudflare, Inc.
Common Name: sni.cloudflaressl.com

Issuer Name:
Country: US
Organization: Cloudflare, Inc.
Common Name: Cloudflare Inc ECC CA-3

Serial Number: 0B 36 FD 5E AF A0 1A 4F A6 3B C1 CF 1C 8C 7C 82

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Jan 25 00:00:00 2023 GMT
Not Valid After: Jan 24 23:59:59 2024 GMT

Public Key Info:
Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 16 82 D1 B1 58 B7 6E A0 5C 49 83 8B AB 5F 04 93 8A 44 66 9F
               EB C8 A0 BC EA 33 D6 7E D5 CD A5 70
Public Key Y: 0E D5 02 03 03 8A CC 2D 08 58 1D 79 21 44 5E 6F 6D FA A9 AF
               8F 34 1A CB 00 35 5E BB 4E 76 24 78
```

Signature Length: 71 bytes / 568 bits
Signature: 00 30 45 02 21 00 D3 0C EE C0 9B 0D A4 C6 BE C0 D0 77 26 04
EE EE B0 48 74 B6 F6 FE 7A C4 05 BE A6 CA 05 C9 5C 87 02 20
49 E1 0F 6E 5E 2E 21 EA 6C A6 51 69 16 FE 3A 0E 16 D2 13 E2
D4 C7 3D 90 D0 F5 5A 4B 6A C6 68 7E

Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: A5 CE 37 EA EB B0 75 0E 94 67 88 B4 45 FA D9 24 10 87 96 1F

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 7A 2E 01 97 3E 08 5D 78 18 BC 76 F3 1F 1D 8B D9 74 3A 0F C5

Extension: Subject Alternative Name (2.5.29.17)
Critical: 0
DNS: 9animes.ph
DNS: sni.cloudflaressl.com
DNS: *.9animes.ph

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)

Extension: CRL Distribution Points (2.5.29.31)
Critical: 0
URI: http://crl3.digicert.com/CloudflareIncECCCA-3.crl
URI: http://crl4.digicert.com/CloudflareIncECCCA-3.crl

Extension: Policies (2.5.29.32)
Critical: 0
Policy ID #1: 2.23.140.1.2.2
Qualifier ID #1: Certification Practice Statement (1.3.6.1.5.5.7 [...])

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=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root
Signature Algorithm : SHA-1 With RSA Encryption
Valid From       : May 12 18:46:00 2000 GMT
Valid To         : May 12 23:59:00 2025 GMT
```

Raw PEM certificate :

-----BEGIN CERTIFICATE-----

MIIDdzCCA1

+gAwIBAgIEAgAAuTANBgkqhkiG9w0BAQUFADBAMQswCQYDVQQGEwJJRTEsMBAGA1UEChMJQmFsdGltb3JlMRMwEQYDVQQLEwpDeWJlc1RydXN0MSIw

+hXe2wCQVt2yguzmKiYv60iNoS6zjrIZ3AQSSBUUnId9Mcyj8e6uYilagnnc

+gRQKfRzMpijS3ljwumUNKoUMMo6vWrJYeKmpYcqWe4PwzV9/lSEy/

CG9VwcPCPwBLKBSua4dnKM3p31vjsufFoREJIE9LAWqSuXmD+tqYF/LTdBlkC1FkYmGPlpWPgkAx9XbIGevOF6uvUA65ehD5f/

xXtabz5OTZydc93Uk3zyZAsuT3lySNTPx8kmCFcB5kpvcY67Oduhjp13RjM71oGDHweI12v/

yej10qhqdNkNwnGjkCAwEAAANFMEMwHQYDVR0OBBYEFOWdWTCR1jMrPoIVDaGezq1BE3wMBIGA1UdEwEB/

wQIMAYBAf8CAQMwDgYDVR0PAQH/BAQDAgEGMA0GCSqGSIb3DQEBBQUAA4IBAQCDFDF2O5G9RaEIFoN27TyclhAO992T9Ldcw46QQF

+vaKSm2eT929hkTI7gQCv1YpNRhcL0EYWoSihfVCr3FvDB81ukMJY2GQE/szKN+OMY3EU/t3WgxjkzSswF07r51XgdIGn9w/

xZchMB5hbgF/X++ZRGjD8ActPhSNzkE1akxehi/oCr0Epn3o0WC4zxe9Z2etciefC7IpJ5OCBRLbflwbWsaY71k5h

+3zvDyny67G7fyUIhzksLi4xaNmjICq44Y3ekQEe5+NauQrz4w1HrQMz2nZQ/1/I6eYs9HRCwBXbsdtTLsr9I4LtD

+gdwyah617jzV/OeBHRnDJELqYzmp

-----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 SHA1	0xC0, 0x09	ECDH	ECDSA	AES-CBC(128)	
ECDHE-ECDSA-AES256-SHA SHA1	0xC0, 0x0A	ECDH	ECDSA	AES-CBC(256)	
ECDHE-ECDSA-AES128-SHA256 SHA256	0xC0, 0x23	ECDH	ECDSA	AES-CBC(128)	
ECDHE-ECDSA-AES256-SHA384 SHA384	0xC0, 0x24	ECDH	ECDSA	AES-CBC(256)	

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: 2023/07/10

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-AES128-SHA256	0xC0, 0x2B	ECDH	ECDSA	AES-GCM(128)	
SHA256					

ECDHE-ECDSA-AES256-SHA384 SHA384	0xC0, 0x2C	ECDH	ECDSA	AES-GCM(256)
ECDHE-ECDSA-CHACHA20-POLY1305 SHA256	0xCC, 0xA9	ECDH	ECDSA	ChaCha20-Poly1305(256)
ECDHE-ECDSA-AES128-SHA SHA1	0xC0, 0x09	ECDH	ECDSA	AES-CBC(128)
ECDHE-ECDSA-AES256-SHA SHA1	0xC0, 0x0A	ECDH	ECDSA	AES-CBC(256)
ECDHE-ECDSA-AES128-SHA256 SHA256	0xC0, 0x23	ECDH	ECDSA	AES-CBC(128)
ECDHE-ECDSA-AES256-SHA384 SHA384	0xC0, 0x24	ECDH	ECDSA	AES-CBC(256)

SSL Version : TLSv11

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	----
ECDHE-ECDSA-AES128-SHA SHA1	0xC0, 0x09	ECDH	ECDSA	AES-CBC(128)	
ECDHE-E [...]					

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-AES128-SHA256	0xC0, 0x2B	ECDH	ECDSA	AES-GCM(128)	
SHA256					
ECDHE-ECDSA-AES256-SHA384	0xC0, 0x2C	ECDH	ECDSA	AES-GCM(256)	
SHA384					
ECDHE-ECDSA-CHACHA20-POLY1305	0xCC, 0xA9	ECDH	ECDSA	ChaCha20-Poly1305(256)	
SHA256					
ECDHE-ECDSA-AES128-SHA	0xC0, 0x09	ECDH	ECDSA	AES-CBC(128)	
SHA1					
ECDHE-ECDSA-AES256-SHA	0xC0, 0x0A	ECDH	ECDSA	AES-CBC(256)	
SHA1					

ECDHE-ECDSA-AES128-SHA256 SHA256	0xC0, 0x23	ECDH	ECDSA	AES-CBC (128)
ECDHE-ECDSA-AES256-SHA384 SHA384	0xC0, 0x24	ECDH	ECDSA	AES-CBC (256)

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\(v=ws.10\)](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=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root
| -Issuer           : C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root
| -Valid From       : May 12 18:46:00 2000 GMT
| -Valid To         : May 12 23:59:00 2025 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
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

<https://ssl-config.mozilla.org/>

Solution

Only enable support for recommended cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2023/07/10

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

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: 2023/07/10

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: 2023/07/10

Plugin Output

tcp/443/www

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

tcp/443/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/8080/www

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


25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

<http://www.ietf.org/rfc/rfc1323.txt>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

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:
```

```
h2
http/1.1
```

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.
```

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: 2023/06/26

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.5.119 to 104.21.28.211 :  
192.168.5.119
```

```
An error was detected along the way.
```

```
An error was detected along the way.
```

```
An error was detected along the way.
```

```
An error was detected along the way.
```

```
An error was detected along the way.
```

```
An error was detected along the way.
```

```
192.168.5.5
```

```
?
```

```
192.168.1.62
```

```
?
```

```
122.15.87.186
```

```
182.19.110.52
```

```
?
```

```
125.18.238.201
```

```
116.119.112.88
```

```
?
```

```
162.158.108.4
```

```
104.21.28.211
```

```
?
```

```
104.21.28.211
```

```
Hop Count: 19
```

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://9animes.ph/lsdceFRuJxIp.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/8080/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://9animes.ph:8080/lsdceFRuJxIp.html
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

Contents of robots.txt :

```
User-agent: *  
Disallow: /wp-admin/  
Allow: /wp-admin/admin-ajax.php  
Sitemap: https://9anim.es.ph/sitemap.xml
```