



MRVA

Report generated by Tenable Nessus™

Fri, 14 Feb 2025 15:06:07 EET

TABLE OF CONTENTS

Vulnerabilities by Host

• 192.168.1.47.....	4
---------------------	---

Nessus Essentials

Vulnerabilities by Host

192.168.1.47



Host Information

DNS Name: linux.home
IP: 192.168.1.47
MAC Address: 08:00:27:AB:4D:CC
OS: Linux Kernel 2.6

Vulnerabilities

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

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

Description

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

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

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

See Also

<https://tools.ietf.org/html/rfc3279>
<http://www.nessus.org/u?9bb87bf2>
<http://www.nessus.org/u?e120eea1>
<http://www.nessus.org/u?5d894816>
<http://www.nessus.org/u?51db68aa>
<http://www.nessus.org/u?9dc7bfba>

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.2

EPSS Score

0.0729

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	11849
BID	33065
CVE	CVE-2004-2761
CVE	CVE-2005-4900
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2009/01/05, Modified: 2023/12/15

Plugin Output

tcp/443/www

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

Subject : CN=www.example.com
Signature Algorithm : SHA-1 With RSA Encryption
Valid From : Sep 16 10:45:03 2015 GMT
Valid To : Sep 13 10:45:03 2025 GMT
Raw PEM certificate :

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

MIIBqzCCARQCCQCsFELirADCzANBgqhkiG9w0BAQUFADAaMRgwFgYDVQQDDA93d3cuZXhhbXBsZS5jb20wHhcNMTUwOTE2MTA0NTAzWhcNMjUwOT
mxwZzBboYF64tu1n8c2zsWOW8FFU0azQFv7RPKcGwtsALkdAMkNcWS7J930xGamdCZPdoRY4hhfesLIshZxpyk6NoYBkmtx
+GfwrrLh6mUyvsyno29GAlqYWffffzXRoibdDtGTn9NeMqXobVTTKTaR0BGspOS5AgMBAAEwDQYJKoZIhvcNAQEFBQADgYEASfG0dH3x4/
XaN6IWwaKo8XeRStjYTy/uBJEBUERlP17X1TooZOYbvgFAqK8DP017EkzASVeu0mS5orfptWjOZ/
UWVZujSNj7uu7QR4vbNERxncZrydr7FklpkIN5Bj8SYc94JI9GsrHip4mpbystXkxncOvESjRBES/iatbk10=
-----END CERTIFICATE-----

91572 - OpenSSL AES-NI Padding Oracle MitM Information Disclosure

Synopsis

It was possible to obtain sensitive information from the remote host with TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability due to an error in the implementation of ciphersuites that use AES in CBC mode with HMAC-SHA1 or HMAC-SHA256. The implementation is specially written to use the AES acceleration available in x86/amd64 processors (AES-NI). The error messages returned by the server allow a man-in-the-middle attacker to conduct a padding oracle attack, resulting in the ability to decrypt network traffic.

See Also

<https://blog.filippo.io/luckyminus20/>

<http://www.nessus.org/u?7647e9f0>

<https://www.openssl.org/news/secadv/20160503.txt>

Solution

Upgrade to OpenSSL version 1.0.1t / 1.0.2h or later.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.1

EPSS Score

0.9702

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	89760
CVE	CVE-2016-2107
XREF	EDB-ID:39768

Plugin Information

Published: 2016/06/13, Modified: 2025/02/11

Plugin Output

tcp/443/www

```
Nessus was able to trigger a RECORD_OVERFLOW alert in the
remote service by sending a crafted SSL "Finished" message.
```


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=www.example.com  
| -Issuer  : CN=www.example.com
```

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=www.example.com

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.

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis

The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Description

At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.

Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

See Also

https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Solution

Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Risk Factor

Low

Plugin Information

Published: 2013/09/03, Modified: 2018/11/15

Plugin Output

tcp/443/www

The following certificates were part of the certificate chain sent by the remote host, but contain RSA keys that are considered to be weak :

```
| -Subject      : CN=www.example.com
| -RSA Key Length : 1024 bits
```


48204 - Apache HTTP Server Version

Synopsis

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

Description

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

See Also

<https://httpd.apache.org/>

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80/www

```
URL      : http://linux.home/
Version  : unknown
Source   : Server: Apache
backported : 0
```

48204 - Apache HTTP Server Version

Synopsis

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

Description

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

See Also

<https://httpd.apache.org/>

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/443/www

```
URL      : https://linux.home/
Version  : unknown
Source   : Server: Apache
backported : 0
```

39446 - Apache Tomcat Detection

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

See Also

<https://tomcat.apache.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0535

Plugin Information

Published: 2009/06/18, Modified: 2024/11/14

Plugin Output

tcp/80/www

```
URL      : http://linux.home/  
Version  : unknown
```

39446 - Apache Tomcat Detection

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

See Also

<https://tomcat.apache.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0535

Plugin Information

Published: 2009/06/18, Modified: 2024/11/14

Plugin Output

tcp/443/www

```
URL      : https://linux.home/  
Version  : unknown
```

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: 2025/02/12

Plugin Output

tcp/0

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

```
cpe:/o:linux:linux_kernel -> Linux Kernel
```

```
Following application CPE's matched on the remote system :
```

```
cpe:/a:apache:http_server -> Apache Software Foundation Apache HTTP Server
```

```
cpe:/a:apache:tomcat -> Apache Software Foundation Tomcat
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 65
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

<https://standards.ieee.org/faqs/regauth.html>

<http://www.nessus.org/u?794673b4>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :
```

```
08:00:27:AB:4D:CC : PCS Systemtechnik GmbH
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:  
- 08:00:27:AB:4D:CC
```


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: 2024/08/09

Plugin Output

tcp/443/www

```
HTTP/1.1 200 OK
Date: Fri, 14 Feb 2025 13:02:07 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Accept-Ranges: bytes
Vary: Accept-Encoding
X-Mod-Pagespeed: 1.9.32.3-4523
Cache-Control: max-age=0, no-cache
Content-Length: 1077
Connection: close
Content-Type: text/html
```

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 :  
Apache
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/443/www

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

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
192.168.1.47 resolves as linux.home.
```

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/1.1 200 OK

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : no

Keep-Alive : yes

Options allowed : (Not implemented)

Headers :

Date: Fri, 14 Feb 2025 13:02:23 GMT

Server: Apache

X-Frame-Options: SAMEORIGIN

Accept-Ranges: bytes

Vary: Accept-Encoding

X-Mod-Pagespeed: 1.9.32.3-4523

Cache-Control: max-age=0, no-cache

Content-Length: 1188

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html

Response Body :

<!doctype 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/1.1 200 OK

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : yes

Keep-Alive : yes

Options allowed : (Not implemented)

Headers :

Date: Fri, 14 Feb 2025 13:02:23 GMT

Server: Apache

X-Frame-Options: SAMEORIGIN

Accept-Ranges: bytes

Vary: Accept-Encoding

X-Mod-Pagespeed: 1.9.32.3-4523

Cache-Control: max-age=0, no-cache

Content-Length: 1077

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html

Response Body :

<!doctype html>

<!--

\ //~~\ | | /\ |~~\~~ | \ /~~\~~|~~ /\ | /~~\ |\ ||~~

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: 2025/02/12

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: 2025/02/12

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: 2024/12/31

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.8.2
Nessus build : 20007
Plugin feed version : 202502130906
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : MRVA
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.1.40
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 237.758 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 : 256
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/2/14 14:59 EET (UTC +02:00)
Scan duration : 421 sec
Scan for malware : no
```

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 : Linux Kernel 2.6  
Confidence level : 65  
Method : SinFP
```

```
The remote host is running Linux Kernel 2.6
```

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

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/02/12

Plugin Output

tcp/0

```
. You need to take the following action :  
[ OpenSSL AES-NI Padding Oracle MitM Information Disclosure (91572) ]  
+ Action to take : Upgrade to OpenSSL version 1.0.1t / 1.0.2h or later.
```

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 TLSv1.0/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 :
```

```
linux.home
```

```
The Common Name in the certificate is :
```

```
www.example.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:

Common Name: www.example.com

Issuer Name:

Common Name: www.example.com

Serial Number: 00 A0 49 F1 0B 8A B0 03 0B

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Sep 16 10:45:03 2015 GMT
Not Valid After: Sep 13 10:45:03 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D9 71 1B FD FC 7B C0 F2 FE 6C 70 67 30 5B A1 81 7A E2 DB
             B5 9F C7 36 CE C5 8E C3 C1 45 53 46 B3 40 5C 6F ED 13 CA 70
             6C 2D B0 02 E4 74 03 24 35 C5 92 EC 9F 77 D3 11 9A 99 D0 99
             3D DA 11 63 88 61 7D EB 0B 22 C8 59 C6 9C A4 E8 DA 18 06 49
             AD C7 E1 9F C2 BA CB 87 A9 94 CA FB 32 9E 8D BD 18 09 6A 61
             67 DF 7F 35 D1 A2 26 DD 0E D1 93 9F D3 5E 32 A5 E8 6D 54 D3
             29 36 91 D0 11 AC A4 E4 B9
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 49 F1 B4 74 7D F1 E3 F5 DA 37 A2 16 C1 A2 A8 F1 77 91 4A
```

Fingerprints :

SHA-1 Fingerprint: EF 0C 5F A5 93 1A 09 A5 68 7C A2 C2 80 C4 C7 92 07 CE F7 1B

PEM certificate :

MIIBQzCCARQCCQcSfEliRADCzANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQDDA93d3cuZXBhbXBzS5jb20wHhcNMTUwOTE2MTA0NTAzWhcNMjUwOTmxwZzBboYF64tu1n8c2zsw0w8FFU0aQZFxv7RPKcGwtsAlkdAMkNcWS7J930xGamdCZPdoRY4hhfesLIshZxpyk6NoYBkmtx+GfwrrLh6mUyvsyno29GAlqYWfff [...]

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-AES128-SHA
SHA1 | 0xC0, 0x13 | ECDH | RSA | AES-CBC(128) | |
| ECDHE-RSA-AES256-SHA
SHA1 | 0xC0, 0x14 | ECDH | RSA | AES-CBC(256) | |
| ECDHE-RSA-AES128-SHA256
SHA256 | 0xC0, 0x27 | ECDH | RSA | AES-CBC(128) | |
| ECDHE-RSA-AES256-SHA384
SHA384 | 0xC0, 0x28 | ECDH | RSA | 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: 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-AES128-SHA256 | 0xC0, 0x2F | ECDH | RSA | AES-GCM(128) | |
| SHA256 | | | | | |
| ECDHE-RSA-AES256-SHA384 | 0xC0, 0x30 | ECDH | RSA | AES-GCM(256) | |
| SHA384 | | | | | |
| ECDHE-RSA-AES128-SHA | 0xC0, 0x13 | ECDH | RSA | AES-CBC(128) | |
| SHA1 | | | | | |
| ECDHE-RSA-AES256-SHA | 0xC0, 0x14 | ECDH | RSA | AES-CBC(256) | |
| SHA1 | | | | | |
| ECDHE-RSA-AES128-SHA256 | 0xC0, 0x27 | ECDH | RSA | AES-CBC(128) | |
| SHA256 | | | | | |
| ECDHE-RSA-AES256-SHA384 | 0xC0, 0x28 | ECDH | RSA | AES-CBC(256) | |
| SHA384 | | | | | |

SSL Version : TLSv11

High Strength Ciphers (>= 112-bit key)

| Name | Code | KEX | Auth | Encryption | MAC |
|------------------------------|------------|------|------|--------------|-----|
| ----- | ----- | --- | ---- | ----- | --- |
| ECDHE-RSA-AES128-SHA
SHA1 | 0xC0, 0x13 | ECDH | RSA | AES-CBC(128) | |
| ECDHE-RSA-AES256-SHA
SHA1 | 0xC0, 0x14 | ECDH | RSA | AES-CBC(256) | |

SSL Version : TLSv1

High Strength Ciphers (>= 112-bit key)

| Name | Code | KEX | Auth | Encryption | MAC |
|------------------------------|------------|------|------|--------------|-----|
| ----- | ----- | --- | ---- | ----- | --- |
| ECDHE-RSA-AES128-SHA
SHA1 | 0xC0, 0x13 | ECDH | RSA | AES-CBC(128) | |
| ECDHE-RSA-AES256-SHA
SHA1 | 0xC0, 0x14 | ECDH | RSA | AES-CBC(256) | |

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
En [...]
```

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-AES128-SHA256 | 0xC0, 0x2F | ECDH | RSA | AES-GCM(128) | |
| SHA256 | | | | | |
| ECDHE-RSA-AES256-SHA384 | 0xC0, 0x30 | ECDH | RSA | AES-GCM(256) | |
| SHA384 | | | | | |
| ECDHE-RSA-AES128-SHA | 0xC0, 0x13 | ECDH | RSA | AES-CBC(128) | |
| SHA1 | | | | | |
| ECDHE-RSA-AES256-SHA | 0xC0, 0x14 | ECDH | RSA | AES-CBC(256) | |
| SHA1 | | | | | |
| ECDHE-RSA-AES128-SHA256 | 0xC0, 0x27 | ECDH | RSA | AES-CBC(128) | |
| SHA256 | | | | | |

| | | | | |
|-------------------------|------------|------|-----|--------------|
| 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}
```

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 recommended 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-AES128-SHA
SHA1 | 0xC0, 0x13 | ECDH | RSA | AES-CBC(128) | |
| ECDHE-RSA-AES256-SHA
SHA1 | 0xC0, 0x14 | ECDH | RSA | AES-CBC(256) | |
| ECDHE-RSA-AES128-SHA256
SHA256 | 0xC0, 0x27 | ECDH | RSA | AES-CBC(128) | |
| ECDHE-RSA-AES256-SHA384
SHA384 | 0xC0, 0x28 | ECDH | RSA | 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}

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 server answered on this port.
```

tcp/443/www

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

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

121010 - TLS Version 1.1 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

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

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

See Also

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

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

Solution

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

Risk Factor

None

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: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.40 to 192.168.1.47 :
192.168.1.40
192.168.1.47

Hop Count: 1
```