universidad full scan

Report generated by Nessus™ Wed, 25 Apr 2018 23:39:34 -05

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

www.unal.edu.co

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	12	1	31

Scan Information

Start time: Wed Apr 25 23:18:00 2018
End time: Wed Apr 25 23:39:33 2018

Host Information

DNS Name: www.unal.edu.co
IP: 168.176.5.69
OS: Linux Kernel 2.6

Vulnerabilities

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: 2018/04/19

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
```

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

```
168.176.5.69 resolves as www.unal.edu.co.
```

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.
- Whether credentialed or third-party patch management checks are possible.
- 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: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 7.0.3
Plugin feed version : 201804251815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.1.17
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
```

```
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2018/4/25 23:18 -05
Scan duration : 1288 sec
```

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: 2011/03/20

Plugin Output

tcp/0

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: 2017/06/06

Plugin Output

tcp/0

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

  cpe:/o:linux:linux_kernel:2.6
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

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

Plugin Output

tcp/0

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

66334 - Patch Report

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.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information:

Published: 2013/07/08, Modified: 2018/04/18

Plugin Output

tcp/0

```
. You need to take the following action :

[ Apache HTTP Server httpOnly Cookie Information Disclosure (57792) ]

+ Action to take : Upgrade to Apache version 2.0.65 / 2.2.22 or later.
```

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: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.17 to 168.176.5.69 :
192.168.1.17
192.168.1.254
10.58.0.1
?
190.240.116.157
190.240.116.158
200.24.33.143
206.223.124.144
10.10.53.30
190.60.96.222
190.60.96.234
168.176.5.69

Hop Count: 11
```

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

http://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:H/RL:OF/RC:C)

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:5648

XREF	OSVDB:11408
XREF	OSVDB:50485
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information:

Published: 2003/01/23, Modified: 2016/11/23

Plugin Output

tcp/80

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus1445350652.html HTTP/1.1
Connection: Close
Host: www.unal.edu.co
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Thu, 26 Apr 2018 04:31:20 GMT
Server: Apache
Keep-Alive: timeout=15, max=500
Connection: Keep-Alive
Content-Type: message/http
Set-Cookie: cookiesession1=006E842CYZBLDS0QBKXIE3TE40GMFFD6;Path=/;HttpOnly
content-length: 317


TRACE /Nessus1445350652.html HTTP/1.1
Connection: Keep-Alive
Host: www.unal.edu.co
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

```
------------------------------ snip ------------------------------
```

57792 - Apache HTTP Server httpOnly Cookie Information Disclosure

Synopsis

The web server running on the remote host is affected by an information disclosure vulnerability.

Description

The version of Apache HTTP Server running on the remote host is affected by an information disclosure vulnerability. Sending a request with HTTP headers long enough to exceed the server limit causes the web server to respond with an HTTP 400. By default, the offending HTTP header and value are displayed on the 400 error page. When used in conjunction with other attacks (e.g., cross-site scripting), this could result in the compromise of httpOnly cookies.

See Also

http://fd.the-wildcat.de/apache_e36a9cf46c.php

http://www.nessus.org/u?e005199a

http://httpd.apache.org/security/vulnerabilities_22.html

http://svn.apache.org/viewvc?view=revision&revision=1235454

Solution

Upgrade to Apache version 2.0.65 / 2.2.22 or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

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

References

BID	51706
CVE	CVE-2012-0053
XREF	OSVDB:78556
XREF	EDB-ID:18442

Plugin Information:

Published: 2012/02/02, Modified: 2017/04/28

Plugin Output

tcp/80

```
Nessus verified this by sending a request with a long Cookie header :

GET / HTTP/1.1
Host: www.unal.edu.co
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

Which caused the Cookie header to be displayed in the default error page
(the response shown below has been truncated) :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
Size of a request header field exceeds server limit.<br />
<pre>
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
```

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

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/80

```
The remote web server type is :

Apache
```

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/wc/exclusion.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

References

XREF OSVDB:238

Plugin Information:

Published: 1999/10/12, Modified: 2014/05/09

Plugin Output

tcp/80

```
Contents of robots.txt :

User-agent: *
Disallow: /stats/
```

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: 2017/05/22

Plugin Output

tcp/80

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

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: 2018/04/24

Plugin Output

tcp/80

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

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: 2017/11/13

Plugin Output

tcp/80

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

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : GET,HEAD,POST,OPTIONS,TRACE
Headers :

  Date: Thu, 26 Apr 2018 04:31:08 GMT
  Server: Apache
  Location: http://unal.edu.co/
  Content-Length: 227
  Keep-Alive: timeout=15, max=500
  Connection: Keep-Alive
  Content-Type: text/html; charset=iso-8859-1

Response Body :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://unal.edu.co/">here</a>.</p>
</body></html>
```

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.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/80

```
URL         : http://www.unal.edu.co/
Version     : unknown
backported : 0
```

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

http://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:H/RL:OF/RC:C)

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:5648

XREF	OSVDB:11408
XREF	OSVDB:50485
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information:

Published: 2003/01/23, Modified: 2016/11/23

Plugin Output

tcp/443

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus813652163.html HTTP/1.1
Connection: Close
Host: www.unal.edu.co
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.0 200 OK
Date: Thu, 26 Apr 2018 04:31:22 GMT
Server: Apache
Connection: close
Content-Type: message/http


TRACE /Nessus813652163.html HTTP/1.1
Connection: Close
Host: www.unal.edu.co
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

15901 - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution

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

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2004/12/03, Modified: 2016/01/08

Plugin Output

tcp/443

```
The SSL certificate has already expired :

  Subject          : C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizationalUnit,
 CN=localhost.localdomain, emailAddress=root@localhost.localdomain
  Issuer           : C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizationalUnit,
 CN=localhost.localdomain, emailAddress=root@localhost.localdomain
  Not valid before : Mar 26 16:35:42 2010 GMT
  Not valid after  : Mar 26 16:35:42 2011 GMT
```

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?0bb7b67d

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.1 (with approved cipher suites) or higher instead.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2005/10/12, Modified: 2017/07/11

Plugin Output

tcp/443

```
- SSLv3 is enabled and the server supports at least one cipher.
```

26928 - SSL Weak Cipher Suites Supported

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer weak encryption.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

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

Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

XREF	CWE:326
XREF	CWE:327
XREF	CWE:720
XREF	CWE:753
XREF	CWE:803
XREF	CWE:928
XREF	CWE:934

Plugin Information:

Published: 2007/10/08, Modified: 2017/09/01

Plugin Output

tcp/443

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

  Low Strength Ciphers (<= 64-bit key)

    EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
    DES-CBC-SHA                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

tcp/443

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

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

    EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
```

```
The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

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

http://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper 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 Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/443

```
The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=localhost.localdomain/E=root@localhost.localdomain
|-Not After : Mar 26 16:35:42 2011 GMT

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=localhost.localdomain/E=root@localhost.localdomain
|-Issuer  : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=localhost.localdomain/E=root@localhost.localdomain
```

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 certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/443

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=localhost.localdomain/E=root@localhost.localdomain
```

57792 - Apache HTTP Server httpOnly Cookie Information Disclosure

Synopsis

The web server running on the remote host is affected by an information disclosure vulnerability.

Description

The version of Apache HTTP Server running on the remote host is affected by an information disclosure vulnerability. Sending a request with HTTP headers long enough to exceed the server limit causes the web server to respond with an HTTP 400. By default, the offending HTTP header and value are displayed on the 400 error page. When used in conjunction with other attacks (e.g., cross-site scripting), this could result in the compromise of httpOnly cookies.

See Also

http://fd.the-wildcat.de/apache_e36a9cf46c.php

http://www.nessus.org/u?e005199a

http://httpd.apache.org/security/vulnerabilities_22.html

http://svn.apache.org/viewvc?view=revision&revision=1235454

Solution

Upgrade to Apache version 2.0.65 / 2.2.22 or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

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

References

BID	51706
CVE	CVE-2012-0053
XREF	OSVDB:78556
XREF	EDB-ID:18442

Plugin Information:

Published: 2012/02/02, Modified: 2017/04/28

Plugin Output

tcp/443

```
Nessus verified this by sending a request with a long Cookie header :

GET / HTTP/1.1
Host: www.unal.edu.co
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

Which caused the Cookie header to be displayed in the default error page
(the response shown below has been truncated) :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
Size of a request header field exceeds server limit.<br />
<pre>
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
```

62565 - Transport Layer Security (TLS) Protocol CRIME Vulnerability

Synopsis

The remote service has a configuration that may make it vulnerable to the CRIME attack.

Description

The remote service has one of two configurations that are known to be required for the CRIME attack :

- SSL / TLS compression is enabled.

- TLS advertises the SPDY protocol earlier than version 4.

Note that Nessus did not attempt to launch the CRIME attack against the remote service.

See Also

http://www.iacr.org/cryptodb/data/paper.php?pubkey=3091

https://discussions.nessus.org/thread/5546

http://www.nessus.org/u?8ec18eb5

https://issues.apache.org/bugzilla/show_bug.cgi?id=53219

Solution

Disable compression and / or the SPDY service.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	55704
BID	55707
CVE	CVE-2012-4929
CVE	CVE-2012-4930
XREF	OSVDB:85926
XREF	OSVDB:85927

Plugin Information:

Published: 2012/10/16, Modified: 2014/09/26

Plugin Output

tcp/443

```
The following configuration indicates that the remote service
may be vulnerable to the CRIME attack :

  - SSL / TLS compression is enabled.
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

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

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	70574
CVE	CVE-2014-3566
XREF	OSVDB:113251
XREF	CERT:577193

Plugin Information:

Published: 2014/10/15, Modified: 2016/11/30

Plugin Output

tcp/443

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.2 (CVSS2#E:F/RL:TF/RC:ND)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808
XREF	OSVDB:91162
XREF	OSVDB:117855

Plugin Information:

Published: 2013/04/05, Modified: 2018/01/29

Plugin Output

tcp/443

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5
    RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

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

Plugin Information:

Published: 2000/01/04, Modified: 2018/03/16

Plugin Output

tcp/443

```
The remote web server type is :

Apache
```

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: 2015/12/30

Plugin Output

tcp/443

```
Subject Name:

Country: --
State/Province: SomeState
Locality: SomeCity
Organization: SomeOrganization
Organization Unit: SomeOrganizationalUnit
Common Name: localhost.localdomain
Email Address: root@localhost.localdomain

Issuer Name:

Country: --
State/Province: SomeState
Locality: SomeCity
Organization: SomeOrganization
Organization Unit: SomeOrganizationalUnit
Common Name: localhost.localdomain
Email Address: root@localhost.localdomain

Serial Number: 1E 47

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 26 16:35:42 2010 GMT
Not Valid After: Mar 26 16:35:42 2011 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 1024 bits
Public Key: 00 E1 C7 61 3B 59 50 BF C5 C2 A7 E4 8C FE E7 6D C8 84 DF F5
            50 C8 8F 5A 83 D5 EF 2B C8 57 63 95 49 21 D2 B3 BD CB BD 99
            D0 E4 A3 54 0F 72 12 A6 0D FA D8 40 3B C2 6B F6 77 CE 0B D8
            E7 BA B3 06 AB 0C 37 E8 8F FD 52 CB 0A A0 E4 34 64 07 CF F3
            31 20 B8 11 8F 0A 29 EA A7 B9 D7 F5 44 D9 32 4F D9 CF BA 09
            0E 3B D8 10 72 06 86 DD 39 84 3C 29 05 FC 01 85 FD B7 46 C1
            B1 3F 86 4A 67 DC 16 E2 5F
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 AB 23 A0 D8 AA 1F A9 10 05 32 34 9E 4E 47 A5 F6 B9 6C 94
           F8 13 AF 86 5C EA 8E 06 58 67 9D DD B8 54 45 A3 5B D8 F8 71
           9C 13 6E DB F4 91 2C 55 7E BA 02 6C 7F EA 1A ED 92 84 3C A6
           E9 CC 54 AA 41 10 D3 60 94 5D 0C B0 42 FE 36 6F 22 34 54 B1
           E4 1B DD AA 26 3B DA C6 8A 14 7A 33 5A 33 56 9A 0F A6 A0 43
           D6 18 59 02 FD 4E D8 F1 7E 91 E7 0E 4A 59 8B 94 9B BB EB 2B
           85 5F B2 69 10 B6 F8 27 D6

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: E7 F8 84 17 12 25 7E 44 9B 88 E4 2D 6F D2 E3 63 37 AD 42 A0


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: E7 F8 84 17 12 25 7E 44 9B 88 E4 2D 6F D2 E3 63 37 AD 42 A0
Country: --
State/Province: SomeState
Locality: SomeCity
Organization: So [...]
```

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: 2017/05/22

Plugin Output

tcp/443

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

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/03/29

Plugin Output

tcp/443

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

SSL Version : TLSv1
  Low Strength Ciphers (<= 64-bit key)

    EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
    DES-CBC-SHA                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

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

    EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1
```

```
SSL Version : SSLv3
  Low Strength Ciphers (<= 64-bit key)

    EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
    DES-CBC-SHA                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

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

    EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au [...]
```

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: 2018/04/24

Plugin Output

tcp/443

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

tcp/443

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

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: 2017/11/13

Plugin Output

tcp/443

```
Response Code : HTTP/1.0 403 Forbidden

Protocol version : HTTP/1.0
SSL : yes
Keep-Alive : no
Options allowed : GET,HEAD,POST,OPTIONS,TRACE
Headers :

  Date: Thu, 26 Apr 2018 04:31:11 GMT
  Server: Apache
  Accept-Ranges: bytes
  Vary: Accept-Encoding,User-Agent
  Content-Length: 5043
  Connection: close
  Content-Type: text/html; charset=UTF-8

Response Body :

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
 <head>
  <title>Apache HTTP Server Test Page powered by CentOS</title>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <style type="text/css">
   body {
    background-color: #fff;
    color: #000;
    font-size: 0.9em;
```

```
    font-family: sans-serif,helvetica;
    margin: 0;
    padding: 0;
   }
   :link {
    color: #0000FF;
   }
   :visited {
    color: #0000FF;
   }
   a:hover {
    color: #3399FF;
   }
   h1 {
    text-align: center;
    margin: 0;
    padding: 0.6em 2em 0.4em;
    background-color: #3399FF;
    color: #ffffff;
    font-weight: normal;
    font-size: 1.75em;
    border-bottom: 2px solid #000;
   }
   h1 strong {
    font-weight: bold;
   }
   h2 {
    font-size: 1.1em;
    font-weight: bold;
   }
   .content {
    padding: 1em 5em;
   }
   .content-columns {
    /* Setting relative positioning allows for
    absolute positioning for sub-classes */
    position: relative;
    padding-top: 1em;
   }
   .content-column-left {
    /* Value for IE/Win; will be overwritten for other browsers */
    width: 47%;
    padding-right: 3%;
    float: left;
    padding-bottom: 2em;
   }
   .content-column-right {
    /* Values for IE/Win; will be overwritten for other browsers */
    width: 47%;
    padding-left: 3%;
    float: left;
    padding-bottom: 2em;
   }
   .content-columns>.content-column-left, .content-columns>.content-column-right {
    /* Non-IE/Win */
   }
   img {
    border: 2px solid #fff;
    padding: 2px;
    margin: 2px;
   }
   a:hover img {
    border: 2px solid #3399FF;
   }
  </style>
 </head>

 <bo [...]
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/12/10, Modified: 2013/05/09

Plugin Output

tcp/443

```
Based on the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /
```

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: 2017/06/05

Plugin Output

tcp/443

```
The host name known by Nessus is :

  www.unal.edu.co

The Common Name in the certificate is :

  localhost.localdomain
```

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.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/443

```
URL        : https://www.unal.edu.co/
Version    : unknown
backported : 0
```

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/02/07, Modified: 2013/10/18

Plugin Output

tcp/443

```
This port supports resuming TLSv1 / SSLv3 sessions.
```

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: 2018/02/15

Plugin Output

tcp/443

```
This port supports SSLv3/TLSv1.0.
```

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

http://www.openssl.org/docs/apps/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: 2017/06/12

Plugin Output

tcp/443

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

  Low Strength Ciphers (<= 64-bit key)

    EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

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

    EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1

The fields above are :
```

```
    {OpenSSL ciphername}
    Kx={key exchange}
    Au={authentication}
    Enc={symmetric encryption method}
    Mac={message authentication code}
    {export flag}
```

62563 - SSL Compression Methods Supported

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

https://tools.ietf.org/html/rfc3749

https://tools.ietf.org/html/rfc3943

https://tools.ietf.org/html/rfc5246

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2012/10/16, Modified: 2018/02/15

Plugin Output

tcp/443

```
Nessus was able to confirm that the following compression method is
supported by the target :

  DEFLATE (0x01)
```

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

http://www.openssl.org/docs/apps/ciphers.html

http://www.nessus.org/u?cc4a822a

http://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/443

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

  Low Strength Ciphers (<= 64-bit key)

    EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
    DES-CBC-SHA                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

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

    EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
```

```
    AES256-SHA                  Kx=RSA      Au=RSA  Enc=AES-CBC(256)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

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). 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: 2015/07/02

Plugin Output

tcp/443

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

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://technet.microsoft.com/en-us/library/cc778623

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: 2016/11/14

Plugin Output

tcp/443

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

|-Subject             : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=localhost.localdomain/E=root@localhost.localdomain
|-Issuer              : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=localhost.localdomain/E=root@localhost.localdomain
|-Valid From          : Mar 26 16:35:42 2010 GMT
|-Valid To            : Mar 26 16:35:42 2011 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

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 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

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.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2018/04/24

Plugin Output

tcp/443

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