basic scan

Report generated by Nessus™ Sun, 15 Oct 2023 22:41:08 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

testfire.net

0	0	3	1	34
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Sun Oct 15 22:03:56 2023
End time: Sun Oct 15 22:41:08 2023

Host Information

DNS Name: testfire.net
IP: 65.61.137.117
OS: Dell EMC VMX, Microsoft Windows Embedded Standard 7

Vulnerabilities

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. 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

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

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

Plugin Information

Published: 2020/11/17, Modified: 2023/06/08

Plugin Output

tcp/443/www

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

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 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.
```

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

See Also

https://weakdh.org/

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

3.2 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.5

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	74733

CVE	CVE-2015-4000
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2015/05/28, Modified: 2022/12/05

Plugin Output

tcp/443/www

```
Vulnerable connection combinations :

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.1
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.1
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)
```

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

https://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information

Published: 2010/04/29, Modified: 2022/08/15

Plugin Output

tcp/0

```
The following hostnames point to the remote host :
  - demo.testfire.net
  - altoromutual.com
```

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: 2023/05/24

Plugin Output

tcp/80/www

```
URL     : http://testfire.net/
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: 2023/05/24

Plugin Output

tcp/443/www

```
URL     : https://testfire.net/
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: 2023/05/24

Plugin Output

tcp/8080/www

```
URL     : http://testfire.net:8080/
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: 2023/09/25

Plugin Output

tcp/0

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

  cpe:/o:microsoft:windows -> Microsoft Windows

Following application CPE matched on the remote system :

  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 : embedded
Confidence level : 59
```

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 :

Apache-Coyote/1.1
```

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-Coyote/1.1
```

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 :

Apache-Coyote/1.1
```

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/1.1 200 OK

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

  Server: Apache-Coyote/1.1
  Content-Type: text/html;charset=ISO-8859-1
  Transfer-Encoding: chunked
  Date: Sun, 15 Oct 2023 16:53:19 GMT
  Connection: close

Response Body :



<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
<head>
<title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
```

```
</head>
<body style="margin-top:5px;">
<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
  <table width="100%" border="0" cellpadding="0" cellspacing="0">
  <tr>
      <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283
 height=80/></a></td>
  <td align="right" valign="top">
    <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</
font></a> | <a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a
 id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="query" id="query" accesskey="S" />
          <input type="submit" value="Go" />
  </td>
  </tr>
  <tr>
  <td align="right" style="background-image:url('/images/
gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt="" width=354
 height=60/></td>
  </tr>
  </table>
</form>
</div>
<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif"
 width=12 height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
 href= [...]
```

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 : GET, HEAD, POST, PUT, DELETE, OPTIONS
Headers :

  Server: Apache-Coyote/1.1
  Content-Type: text/html;charset=ISO-8859-1
  Transfer-Encoding: chunked
  Date: Sun, 15 Oct 2023 16:53:24 GMT
  Connection: close

Response Body :



<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
<head>
<title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
```

```
</head>
<body style="margin-top:5px;">
<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
  <table width="100%" border="0" cellpadding="0" cellspacing="0">
  <tr>
      <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283
 height=80/></a></td>
  <td align="right" valign="top">
    <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</
font></a> | <a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a
 id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="query" id="query" accesskey="S" />
          <input type="submit" value="Go" />
  </td>
  </tr>
  <tr>
  <td align="right" style="background-image:url('/images/
gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt="" width=354
 height=60/></td>
  </tr>
  </table>
</form>
</div>
<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif"
 width=12 height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
 href [...]
```

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/1.1 200 OK

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

  Server: Apache-Coyote/1.1
  Content-Type: text/html;charset=ISO-8859-1
  Transfer-Encoding: chunked
  Date: Sun, 15 Oct 2023 16:53:16 GMT
  Connection: close

Response Body :



<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
<head>
<title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
```

```
</head>
<body style="margin-top:5px;">
<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
  <table width="100%" border="0" cellpadding="0" cellspacing="0">
  <tr>
      <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283
 height=80/></a></td>
  <td align="right" valign="top">
    <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</
font></a> | <a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a
 id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="query" id="query" accesskey="S" />
          <input type="submit" value="Go" />
  </td>
  </tr>
  <tr>
  <td align="right" style="background-image:url('/images/
gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt="" width=354
 height=60/></td>
  </tr>
  </table>
</form>
</div>
<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif"
 width=12 height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
 href= [...]
```

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: 2023/09/25

Plugin Output

tcp/80/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

tcp/443/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

tcp/8080/www

```
Port 8080/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: 2023/07/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.6.1
Nessus build : 20021
Plugin feed version : 202310140610
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : assignment
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.150.4
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 354.583 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 : 2023/10/15 22:04 India Standard Time
Scan duration : 2220 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 : Dell EMC VMX
Microsoft Windows Embedded Standard 7
Confidence level : 59
Method : SinFP


The remote host is running one of these operating systems :
Dell EMC VMX
Microsoft Windows Embedded Standard 7
```

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.
```

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: demo.testfire.net

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 CD 6B 11 69 04 55 82 D2 7C AC 39 7B 69 DA 0C 50

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jun 19 00:00:00 2023 GMT
Not Valid After: Jun 14 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 8D 31 E4 A9 33 54 A3 12 C0 8C A1 7E 19 C8 C5 68 04 91 F8
            8B CD 43 F9 0A 25 DB 12 CA 95 28 A0 79 73 50 D7 D1 1D 8A 8F
            25 4F 61 A6 60 39 36 ED 50 6C DC 67 66 C5 F6 1D B9 C8 CC D4
            71 9A F3 D7 D3 FE D4 00 E3 55 E4 E4 F0 F9 8A 80 58 CC EC B0
            80 DA 66 5D 04 BC CC B7 AE 7C FD 2D 9E DD 36 79 19 DF E8 42
            76 54 A6 E1 EF BB 80 4E CE 30 1C E1 C6 DF 0F 97 D3 B1 38 0D
            7A 03 AD 37 3B 83 42 3A 07 18 2A C9 3B 3E 09 A5 06 83 B9 40
```

```
             9A 2F CD 34 CA 3F FE 8D 47 0E 8E E3 28 17 36 34 6C 2E 38 F8
             CF 3E E1 31 01 07 55 5C 3A 43 CB 36 17 28 16 16 9C 58 12 58
             95 74 B2 59 C9 CC 16 CF E5 AF 26 74 86 1D B8 E0 3E FE C6 3C
             8F 4D 00 4A 3A 0E 4F 7F C8 0B 12 0A DC 87 8F 26 8F 6D 39 7A
             33 BB 36 59 34 95 14 EE 94 CE D9 E2 9A 95 1F 19 75 FE 68 B6
             E6 B9 10 E7 AD CD 62 8A BE C4 E8 D2 AF 62 2F C5 0D
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 C0 AD 30 34 11 F1 FA E6 17 53 0F 49 30 C1 58 E6 17 42 42
           A4 46 88 E5 10 D2 8A 32 E1 C3 54 4E 44 C7 8C F2 A5 8C 62 36
           32 7E 53 0C 11 7F 6B BC 81 22 75 07 83 FE 1E 82 10 DF 01 7D
           2D B2 7A 3A E8 E8 1F D2 32 4A AE 53 D8 74 85 4D FC 77 85 BC
           7E B1 36 8A BF 0F 3C B5 72 3B C0 74 9D 90 31 E0 A9 7A 18 A1
           A5 2E A0 25 B1 EB EE 7C 2B C7 FB B7 FB 72 F0 86 9F 73 41 A6
           76 14 5A 49 DA 49 AB 54 3F 6D 06 2F F9 97 70 51 AF 47 78 97
           2B 47 D0 7F 99 C6 EF 66 CC 64 3 [...]
```

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=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMGh
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgc
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----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
    ----------------------        ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67        DH            RSA      AES-CBC(128)
 SHA256
```

```
    DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
    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}
```

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

    Name                         Code              KEX           Auth     Encryption             MAC
    ----------------------       ----------        ---           ----     --------------------   ---
    DHE-RSA-AES128-SHA256        0x00, 0x9E        DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384        0x00, 0x9F        DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256      0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384      0xC0, 0x30        ECDH          RSA      AES-GCM(256)
 SHA384
    DHE-RSA-AES128-SHA           0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA           0x00, 0x39        DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA         0xC0, 0x13        ECDH          RSA      AES-CBC(128)
 SHA1
```

```
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
    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
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA [...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/443/www

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(256)
 SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
```

```
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
    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}
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/443/www

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

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 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 recommened 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
    ----------------------        ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67        DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B        DH            RSA      AES-CBC(256)
 SHA256
    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}
```

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: 2019/03/06

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: 2023/06/26

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.150.4 to 65.61.137.117 :
192.168.150.4

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.
192.168.150.204
100.64.0.100
192.168.34.205
192.168.48.22
192.168.48.49
122.185.106.217
116.119.61.206
62.115.42.118
62.115.124.56
62.115.122.159
62.115.138.71
?
62.115.136.119
62.115.33.78
?
148.62.41.97
148.62.41.123
74.205.108.69
65.61.137.117
?
65.61.137.117
```

```
Hop Count: 24
```