Testfire Scanning

Wed, 18 Oct 2023 12:56:59 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

65.61.137.117

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	2	1	35

Scan Information

Start time: Wed Oct 18 12:28:21 2023

End time: Wed Oct 18 12:56:59 2023

Host Information

IP: 65.61.137.117

OS: Dell EMC VMX, Microsoft Windows Embedded Standard 7

Vulnerabilities

104743 - TLS Version 1.0 Protocol Detection -

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

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

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

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

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Nessus Essentials

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
```

Nessus Essentials

```
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

Nessus Essentials

Plugin Output

tcp/80/www

```
URL : http://65.61.137.117/
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://65.61.137.117/
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

Nessus Essentials

Plugin Information

Published: 2009/06/18, Modified: 2023/05/24

Plugin Output

tcp/8080/www

```
URL : http://65.61.137.117:8080/
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: 2023/10/16

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

Nessus Essentials

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

Nessus Essentials

```
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
```

Nessus Essentials

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: Wed, 18 Oct 2023 07:13:21 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="/login.jsp" class="focus" >ONLINE
BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?
content=personal.htm" >PERSONAL</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?
content=business.htm" >SMALL BUSINESS</a></div></td>
<td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?
content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
</tr>
<tr>

<!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
<td valign="top" class="cc br bb">
<br style="line-height: 10px;"/>

<a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
<ul class="sidebar">
<li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
<li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
<li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
<li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
<li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
<li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
</ul>

<a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
<ul class="sidebar">
<li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
<li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
<li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
<li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
<li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
<li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
</ul>

<a id="CatLink3" class="subheader" href="index.jsp?content=inside.htm">INSIDE ALTORO MUTUAL</a>
<ul class="sidebar">
<li><a id="MenuHyperLink13" href="index.jsp?content=inside_about.htm">About Us</a></li>
<li><a id="MenuHyperLink14" href="index.jsp?content=inside_contact.htm">Contact Us</a></li>
<li><a id="MenuHyperLink15" href="cgi.exe">Locations</a></li>
<li><a id="MenuHyperLink16" href="index.jsp?content=inside_investor.htm">Investor Relations</a></li>
<li><a id="MenuHyperLink17" href="index.jsp?content=inside_press.htm">Press Room</a></li>
<li><a id="MenuHyperLink18" href="index.jsp?content=inside_careers.htm">Careers</a></li>
<li><a id="MenuHyperLink19" href="subscribe.jsp">Subscribe</a></li>
</ul>
</td>
<!-- TOC END -->

<td valign="top" colspan="3" class="bb">



<!-- Keywords:Altoro Mutual, online banking, banking, checking, savings, accounts -->
<br />
<table border=0 cellspacing=0 width="100%">
<tr>
<td width="33%" valign="top">
<b><a href="index.jsp?content=personal_savings.htm">Online Banking with FREE Online Bill Pay </a></b><br />
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy. <br />
<br />
<center><img src="images/home1.jpg" width="170" height="114" /></center>
<br />

<b><a href="index.jsp?content=personal_loans.htm">Real Estate Financing</a></b><br />
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro
Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the
business, and we have the track record to prove it
</td>
<td width="33%" valign="top">
```

```
<center><img src="images/home2.jpg" width="170" height="128" /></center>
<br /><br/>
<b><a href="index.jsp?content=business_cards.htm">Business Credit Cards</a></b><br />
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and
control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.
<br />

<br />
<b><a href="index.jsp?content=business_retirement.htm">Retirement Solutions</a></b><br />
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through
effective Retirement Solutions.
</td>
<td width="33%" valign="top">
<b>Privacy and Security </b><br />
The 2000 employees of Altoro Mutual are dedicated to protecting your <a href="index.jsp?content=privacy.htm">privacy</a>
and <a href="default.jsp?content=security.htm">security</a>. We pledge to provide you with the information and resources
that you need to help secure your information and keep it confidential. This is our promise.
<br /><br />

<center><img src="images/home3.jpg" width="170" height="113" /></center><br /><br />

<b><a href="survey_questions.jsp">Win a Samsung Galaxy S10 smartphone</a></b>
<br />
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to
hearing your important feedback.
<br /><br />
</td>
</tr>
</table>

</td>

</div>



<!-- BEGIN FOOTER -->


</tr>
</table>
<div id="footer" style="width: 99%;">
<a id="HyperLink5" href="/index.jsp?content=privacy.htm">Privacy Policy</a>
  |  
<a id="HyperLink6" href="/index.jsp?content=security.htm">Security Statement</a>
  |  
<a id="HyperLink6" href="/status_check.jsp">Server Status Check</a>
  |  
<a id="HyperLink6" href="/swagger/index.html">REST API</a>
  |  
&copy; 2023 Altoro Mutual, Inc.
<span style="color:red;font-weight:bold;font-style:italic;float:right">This web application is open source!<span
style="color:black;font-style:italic;font-weight:normal;float:right"> <a
href="https://github.com/AppSecDev/AltoroJ/">Get your copy from GitHub</a> and take advantage of advanced
features</span></span>
<br><br><br>
<div class="disclaimer">
The AltoroJ website is published by IBM Corporation for the sole purpose of
demonstrating the effectiveness of IBM products in detecting web application
vulnerabilities and website defects. This site is not a real banking site. Similarities,
if any, to third party products and/or websites are purely coincidental. This site is
provided "as is" without warranty of any kind, either express or implied. IBM does
not assume any risk in relation to your use of this website. For more information,
please go to <a id="HyperLink7" href="http://www-142.ibm.com/software/products/us/en/subcategory/SWI10" >http://www-
142.ibm.com/software/products/us/en/subcategory/SWI10</a>.<br /><br />

Copyright &copy; 2008, 2023, IBM Corporation, All rights reserved.
</div>
</div>

</body>
</html>
<!-- END FOOTER -->
```

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: Wed, 18 Oct 2023 07:13:25 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="/login.jsp" class="focus" >ONLINE
BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?
content=personal.htm" >PERSONAL</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?
content=business.htm" >SMALL BUSINESS</a></div></td>
<td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?
content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
</tr>
<tr>

<!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
<td valign="top" class="cc br bb">
<br style="line-height: 10px;"/>

<a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
<ul class="sidebar">
<li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
<li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
<li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
<li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
<li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
<li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
</ul>

<a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
<ul class="sidebar">
<li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
<li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
<li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
<li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
<li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
<li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
</ul>

<a id="CatLink3" class="subheader" href="index.jsp?content=inside.htm">INSIDE ALTORO MUTUAL</a>
<ul class="sidebar">
<li><a id="MenuHyperLink13" href="index.jsp?content=inside_about.htm">About Us</a></li>
<li><a id="MenuHyperLink14" href="index.jsp?content=inside_contact.htm">Contact Us</a></li>
<li><a id="MenuHyperLink15" href="cgi.exe">Locations</a></li>
<li><a id="MenuHyperLink16" href="index.jsp?content=inside_investor.htm">Investor Relations</a></li>
<li><a id="MenuHyperLink17" href="index.jsp?content=inside_press.htm">Press Room</a></li>
<li><a id="MenuHyperLink18" href="index.jsp?content=inside_careers.htm">Careers</a></li>
<li><a id="MenuHyperLink19" href="subscribe.jsp">Subscribe</a></li>
</ul>
</td>
<!-- TOC END -->

<td valign="top" colspan="3" class="bb">



<!-- Keywords:Altoro Mutual, online banking, banking, checking, savings, accounts -->
<br />
<table border=0 cellspacing=0 width="100%">
<tr>
<td width="33%" valign="top">
<b><a href="index.jsp?content=personal_savings.htm">Online Banking with FREE Online Bill Pay </a></b><br />
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy. <br />
<br />
<center><img src="images/home1.jpg" width="170" height="114" /></center>
<br />

<b><a href="index.jsp?content=personal_loans.htm">Real Estate Financing</a></b><br />
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro
Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the
business, and we have the track record to prove it
</td>
<td width="33%" valign="top">
<center><img src="images/home2.jpg" width="170" height="128" /></center>
<br /><br/>
<b><a href="index.jsp?content=business_cards.htm">Business Credit Cards</a></b><br />
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and
control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.
<br />

<br />
```

```
<b><a href="index.jsp?content=business_retirement.htm">Retirement Solutions</a></b><br />
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through
effective Retirement Solutions.
</td>
<td width="33%" valign="top">
<b>Privacy and Security </b><br />
The 2000 employees of Altoro Mutual are dedicated to protecting your <a href="index.jsp?content=privacy.htm">privacy</a>
and <a href="default.jsp?content=security.htm">security</a>. We pledge to provide you with the information and resources
that you need to help secure your information and keep it confidential. This is our promise.
<br /><br />

<center><img src="images/home3.jpg" width="170" height="113" /></center><br /><br />

<b><a href="survey_questions.jsp">Win a Samsung Galaxy S10 smartphone</a></b>
<br />
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to
hearing your important feedback.
<br /><br />
</td>
</tr>
</table>

</td>

</div>



<!-- BEGIN FOOTER -->


</tr>
</table>
<div id="footer" style="width: 99%;">
<a id="HyperLink5" href="/index.jsp?content=privacy.htm">Privacy Policy</a>
  |  
<a id="HyperLink6" href="/index.jsp?content=security.htm">Security Statement</a>
  |  
<a id="HyperLink6" href="/status_check.jsp">Server Status Check</a>
  |  
<a id="HyperLink6" href="/swagger/index.html">REST API</a>
  |  
&copy; 2023 Altoro Mutual, Inc.
<span style="color:red;font-weight:bold;font-style:italic;float:right">This web application is open source!<span
style="color:black;font-style:italic;font-weight:normal;float:right"> <a
href="https://github.com/AppSecDev/AltoroJ/">Get your copy from GitHub</a> and take advantage of advanced
features</span></span>
<br><br><br>
<div class="disclaimer">
The AltoroJ website is published by IBM Corporation for the sole purpose of
demonstrating the effectiveness of IBM products in detecting web application
vulnerabilities and website defects. This site is not a real banking site. Similarities,
if any, to third party products and/or websites are purely coincidental. This site is
provided "as is" without warranty of any kind, either express or implied. IBM does
not assume any risk in relation to your use of this website. For more information,
please go to <a id="HyperLink7" href="http://www-142.ibm.com/software/products/us/en/subcategory/SWI10" >http://www-
142.ibm.com/software/products/us/en/subcategory/SWI10</a>.<br /><br />

Copyright &copy; 2008, 2023, IBM Corporation, All rights reserved.
</div>
</div>

</body>
</html>
<!-- END FOOTER -->
```

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: Wed, 18 Oct 2023 07:13:19 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="/login.jsp" class="focus" >ONLINE
BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?
content=personal.htm" >PERSONAL</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?
content=business.htm" >SMALL BUSINESS</a></div></td>
```

```
<td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?
content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
</tr>
<tr>

<!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
<td valign="top" class="cc br bb">
<br style="line-height: 10px;"/>

<a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
<ul class="sidebar">
<li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
<li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
<li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
<li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
<li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
<li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
</ul>

<a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
<ul class="sidebar">
<li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
<li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
<li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
<li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
<li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
<li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
</ul>

<a id="CatLink3" class="subheader" href="index.jsp?content=inside.htm">INSIDE ALTORO MUTUAL</a>
<ul class="sidebar">
<li><a id="MenuHyperLink13" href="index.jsp?content=inside_about.htm">About Us</a></li>
<li><a id="MenuHyperLink14" href="index.jsp?content=inside_contact.htm">Contact Us</a></li>
<li><a id="MenuHyperLink15" href="cgi.exe">Locations</a></li>
<li><a id="MenuHyperLink16" href="index.jsp?content=inside_investor.htm">Investor Relations</a></li>
<li><a id="MenuHyperLink17" href="index.jsp?content=inside_press.htm">Press Room</a></li>
<li><a id="MenuHyperLink18" href="index.jsp?content=inside_careers.htm">Careers</a></li>
<li><a id="MenuHyperLink19" href="subscribe.jsp">Subscribe</a></li>
</ul>
</td>
<!-- TOC END -->

<td valign="top" colspan="3" class="bb">



<!-- Keywords:Altoro Mutual, online banking, banking, checking, savings, accounts -->
<br />
<table border=0 cellspacing=0 width="100%">
<tr>
<td width="33%" valign="top">
<b><a href="index.jsp?content=personal_savings.htm">Online Banking with FREE Online Bill Pay </a></b><br />
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy. <br />
<br />
<center><img src="images/home1.jpg" width="170" height="114" /></center>
<br />

<b><a href="index.jsp?content=personal_loans.htm">Real Estate Financing</a></b><br />
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro
Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the
business, and we have the track record to prove it
</td>
<td width="33%" valign="top">
<center><img src="images/home2.jpg" width="170" height="128" /></center>
<br /><br/>
<b><a href="index.jsp?content=business_cards.htm">Business Credit Cards</a></b><br />
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and
control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.
<br />

<br />
<b><a href="index.jsp?content=business_retirement.htm">Retirement Solutions</a></b><br />
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through
effective Retirement Solutions.
</td>
<td width="33%" valign="top">
<b>Privacy and Security </b><br />
The 2000 employees of Altoro Mutual are dedicated to protecting your <a href="index.jsp?content=privacy.htm">privacy</a>
and <a href="default.jsp?content=security.htm">security</a>. We pledge to provide you with the information and resources
that you need to help secure your information and keep it confidential. This is our promise.
```

```
<br /><br />

<center><img src="images/home3.jpg" width="170" height="113" /></center><br /><br />

<b><a href="survey_questions.jsp">Win a Samsung Galaxy S10 smartphone</a></b>
<br />
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to
hearing your important feedback.
<br /><br />
</td>
</tr>
</table>

</td>

</div>



<!-- BEGIN FOOTER -->


</tr>
</table>
<div id="footer" style="width: 99%;">
<a id="HyperLink5" href="/index.jsp?content=privacy.htm">Privacy Policy</a>
  |  
<a id="HyperLink6" href="/index.jsp?content=security.htm">Security Statement</a>
  |  
<a id="HyperLink6" href="/status_check.jsp">Server Status Check</a>
  |  
<a id="HyperLink6" href="/swagger/index.html">REST API</a>
  |  
&copy; 2023 Altoro Mutual, Inc.
<span style="color:red;font-weight:bold;font-style:italic;float:right">This web application is open source!<span
style="color:black;font-style:italic;font-weight:normal;float:right"> <a
href="https://github.com/AppSecDev/AltoroJ/">Get your copy from GitHub</a> and take advantage of advanced
features</span></span>
<br><br><br>
<div class="disclaimer">
The AltoroJ website is published by IBM Corporation for the sole purpose of
demonstrating the effectiveness of IBM products in detecting web application
vulnerabilities and website defects. This site is not a real banking site. Similarities,
if any, to third party products and/or websites are purely coincidental. This site is
provided "as is" without warranty of any kind, either express or implied. IBM does
not assume any risk in relation to your use of this website. For more information,
please go to <a id="HyperLink7" href="http://www-142.ibm.com/software/products/us/en/subcategory/SWI10" >http://www-
142.ibm.com/software/products/us/en/subcategory/SWI10</a>.<br /><br />

Copyright &copy; 2008, 2023, IBM Corporation, All rights reserved.
</div>
</div>

</body>
</html>
<!-- END FOOTER -->
```

10114 - ICMP Timestamp Request Remote Date Disclosure -

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2023/04/27

Plugin Output

icmp/0

```
The ICMP timestamps seem to be in little endian format (not in network format)
The difference between the local and remote clocks is 1 second.
```

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 : 202310171306
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Testfire Scanning
Scan policy used : Basic Network Scan
Scanner IP : 192.168.1.6
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 277.385 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 : 2023/10/18 12:28 India Standard Time
Scan duration : 1702 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
```

Nessus Essentials

```
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
```

Nessus Essentials

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 3B C2 9A FA 4B 0E D3 E2 DF 75
1B E6 E1 C4 14 EA 07 B6 E9 F1 45 5B B3 61 C2 52 19 60 DD D1
5E 7A 1F 0B F2 5E E8 8C 0F 52 89 6A 47 9A E6 D1 A5 18 4A 43
C3 C0 30 6B EC 00 43 F0 84 D5 9B A5 7F 3E 02 59 4E AB 26 9A
E8 FF D0 77 63 6B C8 56 2F 8C A1 39 CE 26 46 4E 68 B3 B8 EC
37 DE 24 81 E6 B4 D8 8C 55 00 97 C4 B0 4C BD B9 EF

Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 8D 8C 5E C4 54 AD 8A E1 77 E9 9B F9 9B 05 E1 B8 01 8D 61 E1

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 40 0D 7D FB 96 82 31 C3 7F 3E 45 1D 54 93 0D 06 42 4C 4E 4A

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

Extension: Basic Constraints (2.5.29.19)
Critical: 1

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

Extension: Policies (2.5.29.32)
Critical: 0
Policy ID #1: 1.3.6.1.4.1.6449.1.2.2.7
Qualifier ID #1: Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URI: https://sectigo.com/CPS
Policy ID #2: 2.23.140.1.2.1

Extension: Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical: 0
Method#1: Certificate Authority Issuers
URI: http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
Method#2: Online Certificate Status Protocol
URI: http://ocsp.sectigo.com

Extension: 1.3.6.1.4.1.11129.2.4.2
Critical: 0
Data: 04 82 01 69 01 67 00 76 00 76 FF 88 3F 0A B6 FB 95 51 C2 61
CC F5 87 BA 34 B4 A4 CD BB 29 DC 68 42 0A 9F E6 67 4C 5A 3A
74 00 00 01 88 D4 62 39 F2 00 00 04 03 00 47 30 45 02 21 00
C8 3E A6 9F 2A E6 88 7C 4F 69 0A F1 F9 A2 94 67 F8 EF FF A2
1F 2B 59 0F D3 21 19 EC 95 DF A1 6C 02 20 2C C9 9F BB 6E 07
A9 E7 33 44 6F 5E 98 C8 D3 B9 4E 98 FF 76 72 8E 53 CE CF 9E
57 7C 24 56 0A C7 00 75 00 DA B6 BF 6B 3F B5 B6 22 9F 9B C2
BB 5C 6B E8 70 91 71 6C BB 51 84 85 34 BD A4 3D 30 48 D7 FB

```
AB 00 00 01 88 D4 62 3A 50 00 00 04 03 00 46 30 44 02 20 77
6B 9E 0E 02 45 6B 9A 53 E9 3A C7 3F 74 C5 06 5F 0E 9A FD 1B
AC 75 72 5C 08 8A D5 7C FF 2D 94 02 20 4A 31 EB 69 4C 76 21
27 0B 62 42 D4 41 55 9B 58 88 59 FA D8 4A EC 26 B4 C1 4D 44
38 63 BA 76 BB 00 76 00 EE CD D0 64 D5 DB 1A CE C5 5C B7 9D
B4 CD 13 A2 32 87 46 7C BC EC DE C3 51 48 59 46 71 1F B5 9B
00 00 01 88 D4 62 3A 19 00 00 04 03 00 47 30 45 02 20 44 AA
58 54 90 EA 11 32 45 C9 25 ED 93 88 5A 95 33 06 D9 5F E8 7C
F9 3A 95 0D D9 AF FF F8 98 CB 02 21 00 96 01 13 F8 04 FC 82
E5 00 01 00 A0 46 3F 56 11 B7 07 15 0F 22 2A 7A B4 89 A8 11
C1 19 85 14 28


Extension: Subject Alternative Name (2.5.29.17)
Critical: 0
DNS: demo.testfire.net
DNS: altoromutual.com


Fingerprints :

SHA-256 Fingerprint: 16 91 7C 73 38 98 12 75 13 47 1F EE FB B1 30 53 B4 BC 7E 31
F5 CA BE C6 A4 F0 1C 57 AD B6 8E 08
SHA-1 Fingerprint: 5D D2 A3 E5 BA CF 0A 33 94 3A 36 F4 E6 8E 60 E1 BF 28 72 37
MD5 Fingerprint: 11 B3 60 0B C0 35 F1 5E C1 E9 51 0B 3B D8 96 C9


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIGPTCCBSWgAwIBAgIRAM1rEWkEVYLSfKw5e2naDFAwDQYJKoZIhvcNAQELBQAwgY8xCzAJBgNVBAYTAkdCMRswGQYDVQQIExJHcmVhdGVyIE1hbmNoZXN0
ZXIxEDAOBgNVBAcTB1NhbGZvcmQxGDAWBgNVBAoTD1NlY3RpZ28gTGltaXRlZDE3MDUGA1UEAxMuU2VjdGlnbyBSU0EgRG9tYWluIFZhbGlkYXRpb24gU2Vj
dXJlIFNlcnZlciBDQTAeFw0yMzA2MTkwMDAwMDBaFw0yNDA2MTQyMzU5NTlaMBwxGjAYBgNVBAMTEWRlbW8udGVzdGZpcmUubmV0MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAjTHkqTNUoxLAjKF+GcjFaASR+IvNQ/kKJdsSypUooHlzUNfRHYqPJU9hpmA5Nu1QbNxnZsX2HbnIzNRxmvPX0/7UAONV5OTw
+YqAWMzssIDaZl0EvMy3rnz9LZ7dNnkZ3+hCdlSm4e+7gE7OMBzhxt8Pl9OxOA16A603O4NCOgcYKsk7PgmlBoO5QJovzTTKP/6NRw6O4ygXNjRsLjj4zz7h
MQEHVVw6Q8s2FygWFpxYEliVdLJZycwWz+WvJnSGHbjgPv7GPI9NAEo6Dk9/yAsSCtyHjyaPbTl6M7s2WTSVFO6UztnimpUfGXX+aLbmuRDnrc1iir7E6NKv
Yi/FDQIDAQABo4IDBDCCAwAwHwYDVR0jBBgwFoAUjYxexFStiuF36Zv5mwXhuAGNYeEwHQYDVR0OBBYEFEANffuWgjHDfz5FHVSTDQZCTE5KMA4GA1UdDwEB
/wQEAwIFoDAMBgNVHRMBAf8EAjAAMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjBJBgNVHSAEQjBAMDQGCysGAQQBsjEBAgIHMCUwIwYIKwYBBQUH
AgEWF2h0dHBzOi8vc2VjdGlnby5jb20vQ1BTMAgGBmeBDAECATCBhAYIKwYBBQUHAQEEeDB2ME8GCCsGAQUFBzAChkNodHRwOi8vY3J0LnNlY3RpZ28uY29t
L1NlY3RpZ29SU0FEb21haW5WYWxpZGF0aW9uU2VjdXJlU2VydmVyQ0EuY3J0MCMGCCsGAQUFBzABhhdodHRwOi8vb2NzcC5zZWN0aWdvLmNvbTCCAX0GCisG
AQQB1nkCBAIEggFtBIIBaQFnAHYAdv+IPwq2+5VRwmHM9Ye6NLSkzbsp3GhCCp/mZ0xaOnQAAAGI1GI58gAABAMARzBFAiEAyD6mnyrmiHxPaQrx+aKUZ/jv
/6IfK1kP0yEZ7JXfoWwCICzJn7tuB6nnM0RvXpjI07lOmP92co5Tzs+eV3wkVgrHAHUA2ra/az+1tiKfm8K7XGvocJFxbLtRhIU0vaQ9MEjX+6sAAAGI1GI6
UAAABAMARjBEAiB3a54OAkVrmlPpOsc/dMUGXw6a/RusdXJcCIrVfP8tlAIgSjHraUx2IScLYkLUQVWbWIhZ+thK7Ca0wU1EOGO6drsAdgDuzdBk1dsazsVc
t520zROiModGfLzs3sNRSFlGcR+1mwAAAYjUYjoZAAAEAwBHMEUCIESqWFSQ6hEyRckl7ZOIWpUzBtlf6Hz5OpUN2a//+JjLAiEAlgET+AT8guUAAQCgRj9W
EbcHFQ8iKnq0iagRwRmFFCgwLgYDVR0RBCcwJYIRZGVtby50ZXN0ZmlyZS5uZXSCEGFsdG9yb211dHVhbC5jb20wDQYJKoZIhvcNAQELBQADggEBAMCtMDQR
8frmF1MPSTDBWOYXQkKkRojlENKKMuHDVE5Ex4zypYxiNjJ+UwwRf2u8gSJ1B4P+HoIQ3wF9LbJ6OujoH9IySq5T2HSFTfx3hbx+sTaKvw88tXI7wHSdkDHg
qXoYoaUuoCWx6+58K8f7t/ty8Iafc0GmdhRaSdpJq1Q/bQYv+ZdwUa9HeJcrR9B/mcbvZsxkO8Ka+ksO0+LfdRvm4cQU6ge26fFFW7NhwlIZYN3RXnofC/Je
6IwPUolqR5rm0aUYSkPDwDBr7ABD8ITVm6V/PgJZTqsmmuj/0Hdja8hWL4yhOc4mRk5os7jsN94kgea02IxVAJfEsEy9ue8=
-----END CERTIFICATE-----
```

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-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDAdTYWxm
b3JkMRowGAYDVQQKDBFDb21vZG8gQ0EgTGltaXRlZDEhMB8GA1UEAwwYQUFBIENlcnRpZmljYXRlIFNlcnZpY2VzMB4XDTA0MDEwMTAwMDAwMFoXDTI4MTIz
MTIzNTk1OVowezELMAkGA1UEBhMCR0IxGzAZBgNVBAgMEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UEBwwHU2FsZm9yZDEaMBgGA1UECgwRQ29tb2RvIENB
IExpbWl0ZWQxITAfBgNVBAMMGEFBQSBDZXJ0aWZpY2F0ZSBTZXJ2aWNlczCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL5AnfRu4ep2hxxNRUSO
vkbIgwadwSr+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/vg4aijJRPn2jymJBGhCfH
dr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULi
mAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W
8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20v
QUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMGh0dHA6Ly9jcmwuY29tb2RvLm5ldC9BQUFDZXJ0aWZpY2F0ZVNlcnZpY2VzLmNybDANBgkqhkiG
9w0BAQUFAAOCAQEACFb8AvCb6P+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHC
v8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAV
GI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgom7C12yxow+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 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


SSL Version : TLSv1
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

The fields above are :

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

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

Nessus Essentials

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.

Nessus Essentials

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 192.168.1.6 to 65.61.137.117 :
192.168.1.6

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.
192.168.1.1
223.230.16.1
182.71.238.93
182.79.134.105
62.115.42.118
62.115.124.54
62.115.112.242
62.115.125.128
?
62.115.136.119
62.115.33.78
?
148.62.41.103
148.62.41.123
74.205.108.93
65.61.137.117

Hop Count: 18
```

Nessus Essentials

© 2023 Tenable™, Inc. All rights reserved.