Infrastructure - Task #7288

Disable insecure SSL communication on VMs

2015-08-10 16:05 - Chris Jones

Status:	Closed	**Start date:**	2015-08-10
Priority:	Normal	**Due date:**	
Assignee:	Chris Jones	**% Done:**	100%
Category:	Support Operations	**Estimated time:**	0.00 hour
Target version:			
Milestone:	None	**Story Points:**	
Product Version:	*		

Description

Nick pointed out that the following VMs had insecure configurations:
* search-ucsb-1
* cn-dev-ucsb-2
* mn-sandbox-ucsb-2

Change the Apache ssl.conf configuration with:

#SSLCipherSuite HIGH:MEDIUM:!ADH:!MD5

SSLCipherSuite
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES256-GCM-SHA384:AES128-GCM-SHA256:AES256-SHA256:AES128-SHA256:AES256-SHA:AES128-SHA:DES-CBC3-SHA:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!PSK:!RC4

SSLHonorCipherOrder On

SSLProtocol all -SSLv2 -SSLv3

Scan results from UCSB OIT:

Greetings:

Our vulnerability scanner has found a potentially vulnerable host on your network. You should consider taking the recommended actions mentioned in this report in order to reduce the chances of this host being abused by an attacker. If you believe any part of this report to be incorrect, please let us know so that we can work to improve our reporting accuracy.

++
Here is information about potential vulnerabilities that were found:
++

IP: 128.111.54.85
OS: Linux Kernel 3.11
Linux Kernel 3.12
Linux Kernel 3.13
Linux Kernel 3.17
Scanned From: 128.111.12.51 (on-campus address)
Scan Start: Wed Aug 5 11:34:22 2015
Scan End: Wed Aug 5 11:38:23 2015

++

Plugin Name: SSL Version 2 and 3 Protocol Detection (20007)

Synopsis:

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

Description:

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

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

See Also:

http://www.schneier.com/paper-ssl.pdf
http://support.microsoft.com/kb/187498
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70

Solution:

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.1 (with approved cipher suites) or higher instead.

Risk Factor: Medium
CVSS Base Score: 5.0

Plugin Information:

Plugin Output:

Port: 443 / tcp / www

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

++

Plugin Name: SSL RC4 Cipher Suites Supported (65821)

Synopsis:

The remote service supports the use of the RC4 cipher.

Description:

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

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

See Also:

http://www.nessus.org/u?217a3666
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution:

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

Risk Factor: Medium
CVSS Base Score: 4.3
CVSS Temporal Score: 3.7

References:

bid: http://www.securityfocus.com/bid/58796
bid: http://www.securityfocus.com/bid/73684
osvdb: http://osvdb.org/91162
osvdb: http://osvdb.org/117855
cve: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2566
cve: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2808

Plugin Information:

Plugin Output:

Port: 443 / tcp / www
None

++

History

#1 - 2015-08-10 16:19 - Chris Jones

- Status changed from In Progress to Closed

- translation missing: en.field_remaining_hours set to 0.0

- % Done changed from 30 to 100

I've edited /etc/apache2/mods-enabled/ssl.conf, and restarted Apache. I've also done this on cn-dev-unm-2.

#2 - 2015-08-12 03:12 - Chris Jones

- Estimated time set to 0.00

Thanks to Dave's handy check_server_ssl script, I've also disabled SSLv2 and SSLv3 on the following VMs:

- search.test.dataone.org
- knb-test-1.dataone.org
- mn-stage-ucsb-4.dataone.org
- cn-dev-ucsb-1.test.dataone.org
- cn-sandbox-2.test.dataone.org
- cn-sandbox-ucsb-1.test.dataone.org
- cn-sandbox-ucsb-2.test.dataone.org
- mn-demo-1.test.dataone.org
- mn-demo-2.test.dataone.org
- mn-demo-3.test.dataone.org
- mn-demo-4.test.dataone.org
- mn-demo-6.test.dataone.org
- mn-demo-7.test.dataone.org
- mn-demo-8.test.dataone.org
- mn-demo-9.test.dataone.org
- mn-demo-10.test.dataone.org
- mn-demo-11.test.dataone.org
- mn-stage-ucsb-1.test.dataone.org
- mn-stage-ucsb-2.test.dataone.org
- mn-stage-ucsb-3.test.dataone.org
- mn-stage-ucsb-4.test.dataone.org

Note that groups.dataone.org remains to be changed, but I don't have ssh access, so will ask Dave, Nick, or Matt to change it.

#3 - 2015-08-20 03:03 - Chris Jones

- % Done changed from 100 to 30

- Status changed from Closed to In Progress

It seems I missed the cipher suite lines in some of these hosts, so I'm re-opening the ticket. I'll make sure RC4 is disabled:

Greetings:

Our vulnerability scanner has found a potentially vulnerable host on your network. You should consider taking the recommended actions mentioned in this report in order to reduce the chances of this host being abused by an attacker. If you believe any part of this report to be incorrect, please let us know so that we can work to improve our reporting accuracy.

++
Here is information about potential vulnerabilities that were found:
++

IP: 128.111.54.108
OS: Linux Kernel 3.13
Scanned From: 128.111.12.51 (on-campus address)
Scan Start: Mon Aug 17 02:06:54 2015
Scan End: Mon Aug 17 02:07:50 2015

++

Plugin Name: SSL RC4 Cipher Suites Supported (65821)

Synopsis:

The remote service supports the use of the RC4 cipher.

Description:

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

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

#4 - 2015-08-20 15:56 - Chris Jones

- Status changed from In Progress to Closed

- % Done changed from 30 to 100

Okay, I've gone through the list again and made sure the insecure ciphers are disabled on:

search.dataone.org
search.test.dataone.org
knb-test-1.dataone.org
cn-dev-ucsb-1.test.dataone.org
cn-sandbox-ucsb-1.test.dataone.org
cn-sandbox-ucsb-2.test.dataone.org
mn-demo-2.test.dataone.org
mn-demo-3.test.dataone.org
mn-demo-4.test.dataone.org
mn-demo-6.test.dataone.org
mn-demo-7.test.dataone.org
mn-demo-8.test.dataone.org
mn-demo-9.test.dataone.org
mn-demo-10.test.dataone.org
mn-demo-11.test.dataone.org
mn-stage-ucsb-1.test.dataone.org
mn-stage-ucsb-2.test.dataone.org
mn-stage-ucsb-3.test.dataone.org
mn-stage-ucsb-4.test.dataone.org

Should be good to go.