Installer - Bug #23844

Disable SSL 64-bit Block Size Cipher Suites in Apache (SWEET32)

06/07/2018 07:37 AM - Tomer Brisker

Status:	Closed		
Priority:	Normal		
Assignee:	Tomer Brisker		
Category:			
Target version:	1.19.0		
Difficulty:		**Fixed in Releases:**	1.19.0
Triaged:	No	**Found in Releases:**	
Bugzilla link:	1586271	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman-installer/pull/274		

Description

Cloned from https://bugzilla.redhat.com/show_bug.cgi?id=1586271

Description of problem:
Latest release at this time of Satellite (6.3.1) shows vulnerable for sweet32 attack (https://sweet32.info/)

Version-Release number of selected component (if applicable):
Satellite 6.3.1

How reproducible:
Everytime

Steps to Reproduce:
1. nmap -sT -PN -p 443 <SATELLITE> --script=ssl-enum-ciphers.nse
2.
3.

Actual results:
↪ nmap -sT -PN -p 443 satellite.example.com --script=ssl-enum-ciphers.nse

Starting Nmap 7.60 (https://nmap.org) at 2018-06-05 16:08 EDT
Nmap scan report for satellite.example.com (10.13.153.218)
Host is up (0.00051s latency).
rDNS record for 10.10.10.10: satellite.example.com

PORT STATE SERVICE
443/tcp open https | ssl-enum-ciphers: | TLSv1.0: | ciphers: | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A | TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C | TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 2048) - C | TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A | TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A | TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C | compressors: | NULL | cipher preference: server | warnings: | 64-bit block cipher 3DES vulnerable to SWEET32 attack | TLSv1.1: | ciphers: | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A | TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C | TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 2048) - C | TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A | TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A | TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C | compressors: | NULL | cipher preference: server | warnings: | 64-bit block cipher 3DES vulnerable to SWEET32 attack | TLSv1.2: | ciphers: | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A | TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A | TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A | TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA

(secp256r1) - C | TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 2048) - C | TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A | TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A | TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A | TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A | TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A | TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A | TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C | compressors: | NULL | cipher preference: server | warnings: | 64-bit block cipher 3DES vulnerable to SWEET32 attack |_ least strength: C

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds

Expected results:
Satellite 6 not using 3DES cipher

Additional info:

Associated revisions

Revision e89c65e6 - 06/07/2018 09:14 AM - Tomer Brisker

Fixes #23844 - Disable DES ciphers by default

History

#1 - 06/07/2018 07:43 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Assignee set to Tomer Brisker

- Pull request https://github.com/theforeman/foreman-installer/pull/274 added

#2 - 06/07/2018 09:16 AM - Anonymous

- Subject changed from SSL 64-bit Block Size Cipher Suites Supported By Default (SWEET32) to SSL 64-bit Block Size Cipher Suites Supported By Default (SWEET32)

- translation missing: en.field_release set to 353

#3 - 06/07/2018 10:01 AM - Anonymous

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset e89c65e602243134aa533e82bc9c16134d5e44db.

#4 - 07/19/2018 02:49 PM - Ewoud Kohl van Wijngaarden

- Subject changed from SSL 64-bit Block Size Cipher Suites Supported By Default (SWEET32) to Disable SSL 64-bit Block Size Cipher Suites in Apache (SWEET32)

- Triaged set to No

#5 - 07/24/2018 07:35 AM - Tomer Brisker

- Fixed in Releases added

#6 - 08/29/2018 12:20 PM - Ewoud Kohl van Wijngaarden

- Fixed in Releases 1.19.0 added

- Fixed in Releases deleted ()

#7 - 08/29/2018 12:22 PM - Ewoud Kohl van Wijngaarden

- Target version changed from 867 to 1.19.0