Installer - Feature #31387

Tracker # 31386 (Resolved): Default to TLS 1.2+

Disable TLS 1.0 and 1.1 by default in Apache

11/24/2020 04:58 PM - Ewoud Kohl van Wijngaarden

Status:	Closed		
Priority:	Normal		
Assignee:	Ewoud Kohl van Wijngaarden		
Category:	foreman-installer script		
Target version:	2.4.0		
Difficulty:		**Fixed in Releases:**	2.4.0
Triaged:	Yes	**Found in Releases:**	1.24.3
Bugzilla link:		**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman-installer/pull/619		

Description

Clients needing these old versions are going EOL. The ecosystem is ready for TLS 1.2+ by default. This makes it easier for organizations to comply with PCI-DSS and similar stricter policies.

For those that still need older versions, it will be possible to override this via custom-hiera.yaml.

Associated revisions

Revision 06533f71 - 12/17/2020 04:15 PM - Ewoud Kohl van Wijngaarden

Fixes #31387 - Drop TLS 1.0 and TLS 1.1 from Apache

This tightens the defaults on Apache to only accept TLS 1.2+. The platforms that required this are going EOL and this makes it easier to comply with PCI-DSS and similar stricter policies.

History

#1 - 11/24/2020 05:24 PM - The Foreman Bot

- Status changed from New to Ready For Testing

- Assignee set to Ewoud Kohl van Wijngaarden

- Pull request https://github.com/theforeman/foreman-installer/pull/619 added

#2 - 12/12/2020 11:34 PM - Besmir Zanaj

- Found in Releases 1.24.3 added

Having the same issue and system does not pass PCI audit.

What would be the easiest/safest way to disable other than manually changing apache settings?

```
[root@HOST ~]# nmap --script ssl-enum-ciphers -p 443 foreman.domain.com

Starting Nmap 6.40 ( http://nmap.org ) at 2020-12-12 23:28 GMT
Nmap scan report for foreman.domain.com (x.x.x.x)
Host is up (0.0011s latency).
PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   SSLv3: No supported ciphers found
|   TLSv1.0:
|     ciphers:
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
```

```
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 - strong
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 - strong
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 - strong
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 - strong
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 - strong
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA256 - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA256 - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong
```

#3 - 12/15/2020 01:51 PM - Ewoud Kohl van Wijngaarden

- Target version set to 2.4.0

First of all, update to a supported version. Currently that's 2.2 and 2.3. Version 2.0 or 2.1 (I forgot exactly which one) fixes TLS 1.2+ by default for Foreman Proxy. Then you can also add the line from the patch to /etc/foreman-installer/custom-hiera.yaml and rerun the installer.

#4 - 12/17/2020 04:15 PM - The Foreman Bot

- Fixed in Releases 2.4.0 added

#5 - 12/17/2020 05:01 PM - Ewoud Kohl van Wijngaarden

- Status changed from Ready For Testing to Closed

Applied in changeset installer|06533f71557c663fbaad2cc28b93520604c12201.

#6 - 03/19/2021 10:26 AM - Ewoud Kohl van Wijngaarden

- Category changed from Foreman modules to foreman-installer script

- Triaged changed from No to Yes