Installer - Feature #35638

Add stronger ciphers to Candlepin's config

10/17/2022 10:20 AM - Ewoud Kohl van Wijngaarden

Status:	Closed		
Priority:	Normal		
Assignee:	Ewoud Kohl van Wijngaarden		
Category:	Foreman modules		
Target version:	3.5.0		
Difficulty:		**Fixed in Releases:**	3.5.0
Triaged:	Yes	**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/puppet-candlepin/pull/224		

Description

Today the ciphers come from the very first commit (commit:832bafa66c9fdc8d632908613695691e90f78583) and aren't the strongest anymore. In commit:c5a36f728cc12443709d0437b205c4a9e32c0fbe they were changed into a parameter so they can be overridden, but the out of the box experience should be improved.

Reported in https://bugzilla.redhat.com/show_bug.cgi?id=2117265#c1

Associated revisions

Revision 86bb0923 - 10/17/2022 01:26 PM - Ewoud Kohl van Wijngaarden

Fixes #35638 - Update ciphers to be SHA256 or SHA384

In 832bafa66c9fdc8d632908613695691e90f78583 the list was created in the initial commit. Then c5a36f728cc12443709d0437b205c4a9e32c0fbe made it a parameter, but didn't change the values. Since 2013 there are stronger (non-SHA1) ciphers. This is important since the FUTURE crypto policy disallows SHA1 ciphers.

The old ciphers are less secure. In our setup clients talk to Foreman and Foreman talks to Candlepin so this should be safe in terms of compatibility with older clients.

History

#1 - 10/17/2022 10:26 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Assignee set to Ewoud Kohl van Wijngaarden

- Pull request https://github.com/theforeman/puppet-candlepin/pull/224 added

#2 - 10/18/2022 11:52 AM - The Foreman Bot

- Fixed in Releases 3.5.0 added

#3 - 10/18/2022 12:01 PM - Ewoud Kohl van Wijngaarden

- Status changed from Ready For Testing to Closed

Applied in changeset puppet-candlepin|86bb0923677aa7586709ae4266f1c8bf9a1e97c4.

#4 - 11/28/2022 12:17 PM - Ewoud Kohl van Wijngaarden

- Triaged changed from No to Yes