Foreman - Feature #22119

Replace MD5 hashes with SHA

01/02/2018 07:48 PM - Anonymous

Status:	Closed		
Priority:	Normal		
Assignee:	Ivan Necas		
Category:	Security		
Target version:			
Difficulty:		**Fixed in Releases:**	1.20.0
Triaged:	No	**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/6098		

Description

Please see https://github.com/rails/rails/commit/82822a34217503336d51b7baab82cd18cf71e435 for details

Related issues:

Related to Foreman - Tracker #21834: Rails 5.2 upgrade tasks	**Closed**
Related to Katello - Bug #25080: Regenerate VCR casettes after changing the d...	**Closed**
Blocks Foreman - Feature #3511: As a security person, I would like Foreman t...	**Resolved**
Blocks Foreman - Bug #23128: Deface uses MD5 and doesn't work in FIPS-enable ...	**Resolved**

Associated revisions

Revision 1c72a0e1 - 10/03/2018 08:15 AM - Ivan Necas

Fixes #22119 - use SHA instead of MD5 for digesting

MD5 is disabled in FIPS environments.

History

#1 - 01/02/2018 07:48 PM - Anonymous

- Related to Tracker #21834: Rails 5.2 upgrade tasks added

#2 - 10/01/2018 07:57 AM - Ivan Necas

- Blocks Feature #3511: As a security person, I would like Foreman to run in FIPS mode added

#3 - 10/01/2018 09:10 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Assignee set to Ivan Necas

- Pull request https://github.com/theforeman/foreman/pull/6098 added

#4 - 10/01/2018 09:10 AM - Ivan Necas

- Blocks Bug #23128: Deface uses MD5 and doesn't work in FIPS-enable environment added

#5 - 10/01/2018 01:12 PM - Ivan Necas

- Related to Bug #25080: Regenerate VCR casettes after changing the defualt hashing algorithm added

#6 - 10/03/2018 08:15 AM - Marek Hulán

- Category set to Security

- Fixed in Releases 1.20.0 added

#7 - 10/03/2018 09:01 AM - Ivan Necas

- Status changed from Ready For Testing to Closed

Applied in changeset [1c72a0e1cabdccda38ce5802fb0e992a639e09b1](#).