Foreman - Bug #9775

CR encryption key not loaded before it's checked, encryption is disabled

03/16/2015 06:11 AM - Dominic Cleal

Status:	Closed		
Priority:	High		
Assignee:	Dominic Cleal		
Category:	Security		
Target version:	1.8.0		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.8.0
Bugzilla link:	1204914	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/2248		

Description

In Foreman 1.8/nightlies, since #4478, the compute resource password encryption key isn't being used and so CR passwords are stored and loaded only in plain text.

The key is stored in an initialiser (config/initializers/encryption_key.rb, locally generated during package installation) which should be loaded before the Encryptable concern is loaded. The Encryptable concern is a no-op if the key isn't initialised already.

#4478 added config/initializers/apipie.rb which is calling ComputeResource.providers, leading to earlier loading of Encryptable (used in ComputeResource), before the encryption key initialiser is reached (as 'apipie' < 'encryption_key').

Thanks to Daniel Lobato Garcia for reporting this to foreman-security@googlegroups.com.

Related issues:

Related to Foreman - Feature #4478: API docs need to be localized	**Closed**	**02/27/2014**
Related to Foreman - Feature #2424: encrypt compute resource password	**Closed**	**04/24/2013**
Has duplicate Foreman - Bug #9771: undefined method `encryptable_fields' duri...	**Closed**	**03/15/2015**

Associated revisions

Revision 1fcea0e9 - 03/24/2015 04:48 AM - Dominic Cleal

fixes #9775 - always load Encryptable when key's missing, log runtime warning

a59972c3 causes Encryptable to be loaded before the encryption_key.rb
initialiser and the majority of the class was skipped as the key was undefined.

Now Encryptable always loads, but logs at runtime if the key is unavailable,
allowing it to be defined a bit later.

Revision c0429ee2 - 03/26/2015 09:03 AM - Dominic Cleal

fixes #9775 - always load Encryptable when key's missing, log runtime warning

a59972c3 causes Encryptable to be loaded before the encryption_key.rb
initialiser and the majority of the class was skipped as the key was undefined.

Now Encryptable always loads, but logs at runtime if the key is unavailable,
allowing it to be defined a bit later.

(cherry picked from commit 1fcea0e919384f9f0f384d450ecac571d5953c82)

History

#1 - 03/16/2015 06:14 AM - Dominic Cleal

Daniel adds:

- `foreman-rake security:generate_encryption_key` doesn't run by default because of the permissions set by the installer. `Permission denied - /usr/share/foreman/config/initializers/encryption_key.rb`

This works correctly during package installation, it's just a post-install issue that prevents you re-running it. I'll file this separately as it's a low priority and impact bug.

> Before 1.8, I think we should address this. I've naively renamed the initializer to 0_encrypted_key.rb and it fixes the issue. Before 1.8:
>
> - We should document Compute Resource encryption through EncryptionKey in the manual.
> - There should be tests for the tasks that deal with this.
> - Tests for should ensure the initializer runs before the concern is loaded.

Renaming the initialiser certainly works, though as it's a locally created file then we'll need to handle this in packaging somehow - a bit messy. Renaming the apipie initialiser might be easier!

#2 - 03/16/2015 06:22 AM - Dominic Cleal

#9771 is caused by the same issue I believe. The Encryptable concern isn't being loaded due to the initialiser reordering, so the encrypt rake task is failing as the concern methods aren't present.

#4 - 03/16/2015 10:12 AM - Dominic Cleal

- Description updated

- Private changed from Yes to No

#5 - 03/16/2015 10:12 AM - Dominic Cleal

- Related to Feature #4478: API docs need to be localized added

#6 - 03/16/2015 10:12 AM - Dominic Cleal

- Has duplicate Bug #9771: undefined method `encryptable_fields' during db migrate added

#7 - 03/16/2015 10:24 AM - Dominic Cleal

- Related to Feature #2424: encrypt compute resource password added

#8 - 03/16/2015 10:36 AM - Daniel Lobato Garcia

Can confirm #9771 is completely related, as when I make the initializer load earlier it does work.

#9 - 03/19/2015 11:07 AM - Dominic Cleal

- Status changed from New to Assigned

- Assignee set to Dominic Cleal

#10 - 03/20/2015 10:45 AM - The Foreman Bot

- Status changed from Assigned to Ready For Testing

- Pull request https://github.com/theforeman/foreman/pull/2248 added

- Pull request deleted ()

#11 - 03/23/2015 02:16 PM - Og Maciel

- Bugzilla link set to 1204914

#12 - 03/24/2015 05:01 AM - Dominic Cleal

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 1fcea0e919384f9f0f384d450ecac571d5953c82.