Foreman - Bug #6777

CVE-2014-8183 - Models with a 'belongs_to' association to an Organization do not verify association belongs to that Organization

07/24/2014 02:35 PM - Eric Helms

Status:	New		
Priority:	Normal		
Assignee:			
Category:	Organizations and Locations		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:	No	**Found in Releases:**	
Bugzilla link:	1126838	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/1654		

Description

While this affects more models in Katello where every model must be silo'd within an Organization, this problem arises in Foreman as well. Thus, a general use validator that lives in Foreman would be the ideal solution.

Foreman Case:
1. Ensure you have a host and a smart proxy
2. Assign host to organization 'Org A'
3. Assign smart proxy ONLY to organization 'Org B'
4. Ensure 'Org A' does not have any smart proxies
5. Note that UI will not present options to set the Puppet CA for the host on the edit screen
6. Via the API:
PUT to /api/v2/hosts/1 { 'puppet_proxy_id': 1 } (the ID of the smart proxy in 'Org B')
7. Smart proxy that is only in 'Org B' will be assigned to host in 'Org A'

Katello Example:
1. Create Product in 'Org A'
2. Create GPG Key in 'Org B'
3. Via the API:
PUT to /katello/api/v2/products/1 - { 'gpg_key_id': 1} (the ID of the gpg key)
7. Gpg Key from another organization can be assigned to product

History

#1 - 07/28/2014 04:29 AM - Dominic Cleal

- Category set to Organizations and Locations

#2 - 08/05/2014 08:20 AM - Eric Helms

- Bugzilla link set to 1126838

#3 - 08/05/2014 07:41 PM - The Foreman Bot

- Status changed from New to Ready For Testing

- Target version set to 1.7.5

- Pull request https://github.com/theforeman/foreman/pull/1654 added

- Pull request deleted ()

#4 - 08/20/2014 06:50 AM - Anonymous

- Target version changed from 1.7.5 to 1.7.4

#5 - 09/10/2014 07:21 AM - Anonymous

- Target version changed from 1.7.4 to 1.7.3

#6 - 09/30/2014 10:48 AM - Dominic Cleal

- Target version changed from 1.7.3 to 1.7.2

#7 - 04/05/2016 09:56 AM - Tomer Brisker

- Status changed from Ready For Testing to New

#8 - 08/15/2017 04:15 AM - Tomer Brisker

- Subject changed from Models with a 'belongs_to' association to an Organization do not verify association belongs to that Organization to CVE-2014-8183 - Models with a 'belongs_to' association to an Organization do not verify association belongs to that Organization

#9 - 07/23/2018 11:27 AM - Tomer Brisker

- Target version deleted (1.7.2)