Foreman - Bug #15268

CVE-2016-4475 - API and UI org/locations actions not limited to user's associated orgs/locations

06/02/2016 08:59 AM - Dominic Cleal

Status:	Closed		
Priority:	High		
Assignee:	Marek Hulán		
Category:	Security		
Target version:	1.11.4		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1342665	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/3568, https://github.com/Katello/katello/pull/6129		

Description

A number of API and UI actions/URLs for viewing and managing organisations and locations are not limited to the orgs/locations assigned directly to the user, instead they are only restricted by permissions assigned to the user's roles.

- API index calls: GET /api/v2/organizations, GET /api/v2/locations
- API show/update/destroy calls
- UI edit/update/destroy calls

The UI index for orgs/locations and the UI org/location switcher appears to be the only place where the user's associated orgs/locations are taken into account.

Both UI and API controllers should be overriding methods for resource scopes to limit them further to the Organization.my_organizations/Location.my_locations scopes.

Mitigation: ensure all org/location related permissions assigned to a user are restricted to certain orgs/locations, these should still be taken into account.

Thanks to Ivan Necas for reporting this to foreman-security@googlegroups.com.

Related issues:

Related to Foreman - Tracker #10022: Taxonomies related issues	**New**	**04/05/2015**

Associated revisions

Revision a30ab44e - 06/23/2016 02:36 AM - Marek Hulán

Fixes #15268 - limit user taxonomies using my scopes

Fixes CVE-2016-4475

Revision 399bb10b - 07/01/2016 08:12 AM - Marek Hulán

Fixes #15268 - limit user taxonomies using my scopes

Fixes CVE-2016-4475

(cherry picked from commit a30ab44ed6f140f1791afc51a1e448afc2ff28f9)

Revision 7d908032 - 07/22/2016 09:43 AM - Marek Hulán

Fixes #15268 - limit user taxonomies using my scopes

Fixes CVE-2016-4475

(cherry picked from commit a30ab44ed6f140f1791afc51a1e448afc2ff28f9)

History

#1 - 06/02/2016 10:36 AM - Marek Hulán

- Status changed from New to Assigned

- Assignee set to Marek Hulán

#2 - 06/02/2016 11:08 AM - Marek Hulán

- Related to Tracker #10022: Taxonomies related issues added

#3 - 06/02/2016 11:37 AM - The Foreman Bot

- Status changed from Assigned to Ready For Testing

- Pull request https://github.com/theforeman/foreman/pull/3568 added

#4 - 06/03/2016 05:35 AM - Dominic Cleal

- Subject changed from API and UI org/locations actions not limited to user's associated orgs/locations to CVE-2016-4475 - API and UI org/locations actions not limited to user's associated orgs/locations

#5 - 06/03/2016 03:53 PM - Bryan Kearney

- Bugzilla link set to 1342665

#6 - 06/16/2016 05:01 AM - The Foreman Bot

- Pull request https://github.com/Katello/katello/pull/6129 added

#7 - 06/21/2016 03:46 AM - Dominic Cleal

- translation missing: en.field_release changed from 159 to 169

#8 - 06/23/2016 03:01 AM - Marek Hulán

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset a30ab44ed6f140f1791afc51a1e448afc2ff28f9.