Foreman - Bug #15182

CVE-2016-4451 - Privileges escalation through Organization and Locations API

05/25/2016 10:26 AM - Marek Hulán

Status:	Closed		
Priority:	Normal		
Assignee:	Marek Hulán		
Category:	Security		
Target version:	1.11.3		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1340107	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/3553		

Description

We set current org/loc for user in before filter blindly without any association check [2][3]. As a user I'd expect 404 (bug fixed by #3549) but I get the list of resources from org I've chosen even though I'm not associated to it.

Note that this is possible because users have by default viewer_role allowing to view all data regardless of organization. If user would have all filters associated to org 1 only he/she wouldn't see resource from org 2.

[2]https://github.com/theforeman/foreman/blob/develop/app/controllers/concerns/api/taxonomy_scope.rb#L11
[3]https://github.com/theforeman/foreman/blob/develop/app/controllers/concerns/api/taxonomy_scope.rb#L14

Related issues:

Related to Foreman - Bug #2524: Taxonomy scope API parameters not documented	**Closed**	**05/21/2013**
Related to Foreman - Tracker #10022: Taxonomies related issues	**New**	**04/05/2015**

Associated revisions

Revision 1144040f - 05/27/2016 07:34 AM - Marek Hulán

Fixes #15182 - limit user taxonomies in API (CVE-2016-4451)

Revision c4cdec71 - 06/16/2016 02:15 PM - Marek Hulán

Fixes #15182 - limit user taxonomies in API (CVE-2016-4451)

(cherry picked from commit 1144040f444b4bf4aae81940a150b26b23b4623c)

History

#1 - 05/25/2016 10:28 AM - Marek Hulán

- Related to Bug #2524: Taxonomy scope API parameters not documented added

#2 - 05/25/2016 10:28 AM - Marek Hulán

- Status changed from New to Assigned

present probably since 1.7

#3 - 05/25/2016 10:42 AM - Marek Hulán

- Related to Tracker #10022: Taxonomies related issues added

#4 - 05/25/2016 11:48 AM - The Foreman Bot

- Status changed from Assigned to Ready For Testing

- Pull request https://github.com/theforeman/foreman/pull/3553 added

#5 - 05/26/2016 09:00 AM - Marek Hulán

- Subject changed from Privileges escalation through Organization and Locations API to CVE-2016-4451 - Privileges escalation through Organization

and Locations API

#6 - 05/26/2016 09:09 AM - Marek Hulán

- Bugzilla link set to 1340107

#7 - 05/27/2016 08:02 AM - Marek Hulán

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 1144040f444b4bf4aae81940a150b26b23b4623c.