Foreman - Bug #16982

CVE-2016-7078 - User with no organizations or locations can see all resources

10/18/2016 06:23 AM - Daniel Lobato Garcia

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Daniel Lobato Garcia</td>
</tr>
<tr>
<td>Category:</td>
<td>Security</td>
</tr>
<tr>
<td>Target version:</td>
<td>1.15.0</td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Pull request:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://github.com/theforeman/foreman/pull/4329">https://github.com/theforeman/foreman/pull/4329</a>,</td>
</tr>
<tr>
<td></td>
<td><a href="https://github.com/theforeman/foreman/pull/3961">https://github.com/theforeman/foreman/pull/3961</a>,</td>
</tr>
<tr>
<td></td>
<td><a href="https://github.com/theforeman/foreman/pull/4172">https://github.com/theforeman/foreman/pull/4172</a>,</td>
</tr>
<tr>
<td></td>
<td><a href="https://github.com/theforeman/foreman/pull/4327">https://github.com/theforeman/foreman/pull/4327</a>,</td>
</tr>
<tr>
<td></td>
<td><a href="https://github.com/theforeman/foreman/pull/4328">https://github.com/theforeman/foreman/pull/4328</a>,</td>
</tr>
<tr>
<td></td>
<td><a href="https://github.com/theforeman/foreman/pull/3954">https://github.com/theforeman/foreman/pull/3954</a></td>
</tr>
<tr>
<td>Triaged:</td>
<td></td>
</tr>
<tr>
<td>Bugzilla link:</td>
<td></td>
</tr>
<tr>
<td>Fixed in Releases:</td>
<td></td>
</tr>
<tr>
<td>Found in Releases:</td>
<td></td>
</tr>
</tbody>
</table>

Description
The default scope for hosts does not restrict properly by taxonomies. Given this use case:

1. User has role 'Edit host'
2. User has no organization or location
3. User logs in, goes to /hosts and can do anything it's permissions allow to. The list of hosts is unrestricted and shows hosts in any location or organization.
4. If the user gets a taxonomy assigned to it, then the restriction works normally.

This should work so that:

- Users without taxonomies, when set to 'any context' cannot see anything
- Users with taxonomies, when set to 'any context' can see everything within all of their taxonomies context.
- Admins set to 'any context' can see everything - regardless of whether it has a taxonomy or not.
- Users or admins set to some organization/location scope can only see stuff within scope.

Pending CVE number.

Related issues:
- Related to Foreman - Bug #18662: Ensure Taxonomix empty default scope isn't o... Closed 02/24/2017
- Related to Discovery - Bug #18688: Fix broken tests after taxonomy scope change Closed 02/27/2017
- Related to Discovery - Bug #19409: Auto provision does not work after taxonom... Closed 04/27/2017
- Related to Foreman - Bug #20017: Mail notifications not being sent Closed 06/14/2017
- Related to Foreman - Bug #20321: Cannot use foreman-rake import:puppet_classes... Closed 07/17/2017
- Related to Foreman - Bug #20515: User searching by login in code does not fin... Closed 08/07/2017
- Copied to Katello - Bug #17266: Fix tests that depend on CVE 2016-7078 Closed 10/18/2016

Associated revisions
Revision 5f606e11 - 02/22/2017 03:26 AM - Daniel Lobato Garcia
Fixes #16982 - Scope properly when no taxonomies are set

05/09/2020
The default scope for hosts and other objects did not restrict properly by taxonomies. An user without organizations or locations, could do anything it's permissions allow to. The list of hosts was unrestricted and showed hosts in any location or organization.

This is fixed to work so that:

Users without taxonomies, when set to 'any context' cannot see anything (at all)

Users with taxonomies, when set to 'any context' can see everything within all of their taxonomies context (including children taxonomies).

Admins set to 'any context' can see everything - regardless of whether it has a taxonomy or not.

Users or admins set to some organization/location scope can only see stuff within scope.

Revision 0804d857 - 02/24/2017 10:07 AM - Dominic Cleal
refs #16982 - pass ID, not models into model.find

Revision f16b2068 - 02/26/2017 09:10 AM - Dominic Cleal
refs #16982 - remove User.current deassignment (no such user)

Allows the scope change to be reverted, as User.current is no longer set to `nil` (there is no `admin` user).

This was relying on a bug in Ruby on Rails 4.2 where the `unscoped` call filtered through thread variables into Subnet.subnet_for which calls Subnet.all. This is fixed in 5.0, so the user must be set correctly.

Revision 52bae9f0 - 02/27/2017 04:15 PM - Dominic Cleal
refs #16982 - check _ids getters as admin user in taxonomy tests

After a request and User.current is back to nil, the _ids getters will not return any results as the default taxonomix scopes don't permit it. The clone test was instead testing that _no records were associated.
Revision 777fecc6 - 04/27/2017 10:56 AM - Ohad Levy
fixes #19409 - auto provision now uses anonymous admin (#342)

with the introduction of Bug fix #16982: CVE-2016-7078 - User with no organizations or locations can see all resources added.
Discovery queries without a current user fail, this fixes that.

History

#1 - 10/18/2016 10:05 AM - Dominic Cleal
- Subject changed from User with no taxonomies can see all hosts to CVE-2016-7078 - User with no organizations or locations can see all hosts
- Status changed from New to Assigned

#2 - 10/18/2016 10:09 AM - Dominic Cleal
- Subject changed from CVE-2016-7078 - User with no organizations or locations can see all hosts to CVE-2016-7078 - User with no organizations or locations can see all resources

Applies to both hosts and objects linked to multiple orgs/locs (via Taxonomix).

#3 - 10/19/2016 05:34 AM - The Foreman Bot
- Status changed from Assigned to Ready For Testing
- Pull request https://github.com/theforeman/foreman/pull/3954 added

#4 - 10/21/2016 03:25 PM - The Foreman Bot
- Pull request https://github.com/theforeman/foreman/pull/3961 added

#5 - 11/04/2016 12:46 PM - Daniel Lobato Garcia
- Target version set to 1.5.2

#6 - 11/08/2016 04:48 AM - Daniel Lobato Garcia
- Copied to Bug #17266: Fix tests that depend on CVE 2016-7078 added

#7 - 11/15/2016 10:03 AM - Daniel Lobato Garcia
- Target version changed from 1.5.2 to 1.4.3

#8 - 01/10/2017 03:38 PM - The Foreman Bot
- Pull request https://github.com/theforeman/foreman/pull/4172 added

#9 - 01/24/2017 09:57 AM - Daniel Lobato Garcia
- Target version changed from 1.4.3 to 169

#10 - 02/18/2017 10:23 AM - Brad Buckingham
- Target version deleted (169)

#11 - 02/21/2017 09:52 AM - Daniel Lobato Garcia
- Target version set to 1.11.0

#12 - 02/22/2017 04:01 AM - Anonymous
- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100
#13 - 02/22/2017 06:49 AM - Dominic Cleal
- Legacy Backlogs Release (now unused) set to 209

#14 - 02/24/2017 07:13 AM - The Foreman Bot
- Pull request https://github.com/theforeman/foreman/pull/4327 added

#15 - 02/24/2017 07:14 AM - The Foreman Bot
- Pull request https://github.com/theforeman/foreman/pull/4328 added

#16 - 02/24/2017 07:21 AM - The Foreman Bot
- Pull request https://github.com/theforeman/foreman/pull/4329 added

#17 - 02/24/2017 07:46 AM - Dominic Cleal
- Related to Bug #18662: Ensure Taxonomix empty default scope isn't overridden by association scopes added

#18 - 02/27/2017 02:47 AM - Lukas Zapletal
- Related to Bug #18686: Fix broken tests after taxonomy scope change added

#19 - 04/27/2017 05:04 AM - Lukas Zapletal
- Related to Bug #19313: Auto-provisioning does not orchestrate TFTP added

#20 - 04/27/2017 06:27 AM - Ohad Levy
- Related to Bug #19409: Auto provision does not work after taxonomy fix added

#21 - 05/03/2017 04:47 AM - Lukas Zapletal
- Related to deleted (Bug #19313: Auto-provisioning does not orchestrate TFTP)

#22 - 06/14/2017 07:23 AM - Marek Hulán
- Related to Bug #20017: Mail notifications not being sent added

#23 - 07/18/2017 08:57 AM - Marek Hulán
- Related to Bug #20321: Cannot use foreman-rake import:puppet_classes on Foreman 1.15.1/Katello 3.4.2 added

#24 - 08/07/2017 09:33 AM - Marek Hulán
- Related to Bug #20515: User searching by login in code does not find the user because of missing unscoped added