Discovery - Bug #10005
CVE-2015-1844 - Discovery hosts are not restricted to user taxonomies
04/02/2015 09:44 AM - Marek Hulán

<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>Lukas Zapletal</td>
</tr>
<tr>
<td>Category:</td>
<td>Discovery plugin</td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td>Pull request: <a href="https://github.com/theforeman/foreman_discovery/pull/177">https://github.com/theforeman/foreman_discovery/pull/177</a></td>
</tr>
<tr>
<td>Triaged:</td>
<td>No</td>
</tr>
<tr>
<td>Bugzilla link:</td>
<td>Fixed in Releases:</td>
</tr>
</tbody>
</table>

**Description**

I found security issue that's very similar to what is being fixed in Foreman and tracked as [http://projects.theforeman.org/issues/9947](http://projects.theforeman.org/issues/9947). The Foreman fix doesn't fix it, because it's present in discovery codebase. See [https://github.com/theforeman/foreman_discovery/blob/develop/app/models/host/discovered.rb#L30](https://github.com/theforeman/foreman_discovery/blob/develop/app/models/host/discovered.rb#L30)

This allows user to manipulate all discovered hosts (if they have global permission) even if they are assigned to specific org/loc. The fix is either to apply the same patch as we did in Foreman Host::Managed or (better) move the fix to Host::Base and remove this default scope from discovery.

**Related issues:**

- Related to Foreman - Refactor #10025: Move taxonomy related methods and scope... Closed 04/06/2015
- Related to Foreman - Bug #9947: CVE-2015-1844 - GET /api/hosts doesn't respec... Closed 03/30/2015

**Associated revisions**

- Revision c2e61ec2 - 04/19/2015 06:19 AM - Lukas Zapletal
  Fixes #10005 - removed unused default scope and added tax tests

**History**

**#2 - 04/02/2015 10:05 AM - Marek Hulán**

Yes, core bug is public. I'd wait with public PR until confirmed by others. I don't see a point why to duplicate this default_scope. Host::Base already has notion of taxonomies [https://github.com/theforeman/foreman/blob/develop/app/models/host/base.rb#L202](https://github.com/theforeman/foreman/blob/develop/app/models/host/base.rb#L202). Of course belongs_to $taxonomy should be moved to Base as well...

**#3 - 04/02/2015 10:09 AM - Dominic Cleal**

Small reminder - please don't mark notes as private within a private bug, all will be private automatically. It also means when the bug is made public, discussion will be visible.

**#4 - 04/03/2015 03:53 AM - Lukas Zapletal**

From comment 1: "I am against moving it to Host::Base that could be quite confusing. I will do the same patch in Host::Discovered."

Since Host::Base already contains that, I agree this would be good fit. Can you refactor this please? I will test this with Discovery plugin.

**#5 - 04/06/2015 03:18 AM - Marek Hulán**

Btw even if we move the taxonomy related stuff into Host::Base, you should probably prepare a patch that fixes the default scope in discovery for older versions. The move to Host::Base won't be backported. And after the move you still have to remove default_scope so it does not redefine the one from Base.
- Related to Refactor #10025: Move taxonomy related methods and scopes to Host::Base added

Lzap you can test with [https://github.com/theforeman/foreman/pull/2287](https://github.com/theforeman/foreman/pull/2287)

- Related to Bug #9947: CVE-2015-1844 - GET /api/hosts doesn't respect organization/location membership added

This is being handled as a continuation of CVE-2015-1844, specifically targeting Foreman Discovery.

- Private changed from Yes to No

#10 - 04/13/2015 05:59 AM - Dominic Cleal
- Subject changed from Discovery hosts are not restricted to user taxonomies to CVE-2015-1844 - Discovery hosts are not restricted to user taxonomies

The code there hasn't changed from 1.5 release, no need of backports there really.

#13 - 04/19/2015 07:01 AM - Anonymous
- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100

Applied in changeset foreman_discovery/c2e61ec2c8fc00ed90588334ceedce6006db97bf.

#14 - 04/20/2015 05:20 AM - Dominic Cleal
Lukas Zapletal wrote:

- The code there hasn't changed from 1.5 release, no need of backports there really.

If it hasn't changed, then perhaps we do need to backport it to 2.x?
Dominic Cleal wrote:

Lukas Zapletal wrote:

The code there hasn't changed from 1.5 release, no need of backports there really.

If it hasn't changed, then perhaps we **do** need to backport it to 2.x?

I have tested discovery 2.0 and it is not affected.

---

#16 - 04/20/2015 08:36 AM - Dominic Cleal

Lukas Zapetal wrote:

Dominic Cleal wrote:

Lukas Zapetal wrote:

The code there hasn't changed from 1.5 release, no need of backports there really.

If it hasn't changed, then perhaps we **do** need to backport it to 2.x?

I have tested discovery 2.0 and it is not affected.

Ok, was that with the [#10025](#10025) patch on 1.7-stable or without?

I know 3.x has gained some taxonomy features, but did they introduce an issue here somehow?
Okay let me explain this with a table. I covered the following:

<table>
<thead>
<tr>
<th>Foreman version</th>
<th>Discovery version</th>
<th>Patch applied</th>
<th>Vulnerable</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.7</td>
<td>2.0</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1.7</td>
<td>2.0</td>
<td>Yes</td>
<td>Not tested</td>
</tr>
<tr>
<td>1.8</td>
<td>3.0</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>1.8</td>
<td>3.0</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Since the bug #9947 is scheduled for 1.7 and since there were no changes in regard to taxonomy between 2.0 and 3.0 versions, I don't believe it's vulnerable. HAVENT TESTED THO. The patch does not apply cleanly.

I've verified 1.7/2.0 with patch applied, NOT vulnerable. It works, we need the core patch in 1.7.