**Foreman - Bug #16971**

**CVE-2016-7077 - Association lists (for < 6 items) shown without authorization/filters**

10/17/2016 10:38 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>Marek Hulán</td>
</tr>
<tr>
<td>Category:</td>
<td>Security</td>
</tr>
<tr>
<td>Target version:</td>
<td>1.14.0</td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
</tbody>
</table>

| Pull request: | https://github.com/theforeman/foreman/pull/3955 |
| Fixed in Releases: | |
| Found in Releases: | |

**Description**

To reproduce:

1. setup user with permissions to create architectures
2. make sure you have less than 6 OS in Foreman
3. login as that user, try to create architecture
4. you can see all OSes listed there even if the user does not have any OS permission

Note that when there are 6 or more OSes, association is authorized properly.

The code that's responsible for this can be found at [1]. I believe it's present since Foreman 1.1 [2]. Since this is in generic helper, each form using this helper is vulnerable. It looks like the `>= 6` code path (via `multiple_select`) had authorization implemented in [7337] for 1.9.0, and the `< 6` code path was left untouched.

[2] https://github.com/theforeman/foreman/commit/14d225cc561b6fb2678eb87e9323d7750a06195c

**Related issues:**

Related to Foreman - Bug #17256: Non-admin user can't edit his own profile if... Closed 11/07/2016

**Associated revisions**

Revision caffb7e8 - 11/09/2016 05:30 AM - Marek Hulán

Fixes #16971 - CVE-2016-7077 remove unauthorized checkboxes

**History**

#1 - 10/17/2016 10:42 AM - Marek Hulán
- Legacy Backlogs Release (now unused) set to 189

#2 - 10/18/2016 10:07 AM - Dominic Cleal
- Subject changed from Associations are not authorized if resource count is less than 6 to CVE-2016-7077 - Association lists (for < 6 items) shown without authorization/filters
- Status changed from New to Assigned

#3 - 10/18/2016 10:32 AM - Marek Hulán
- Target version changed from 1.5.0 to 1.4.2

#4 - 10/19/2016 06:49 AM - The Foreman Bot
- Status changed from Assigned to Ready For Testing
- Pull request https://github.com/theforeman/foreman/pull/3955 added
#5 - 11/07/2016 12:04 PM - Marek Hulán
- Related to Bug #17256: Non-admin user can't edit his own profile if he has more than 5 roles added

#6 - 11/08/2016 09:35 AM - Marek Hulán
- Target version changed from 1.4.2 to 1.4.4

#7 - 11/09/2016 06:01 AM - Anonymous
- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100

Applied in changeset cafb7e8a60004c9c55b6d94f767be33046f372.