Foreman - Bug #19612
CVE-2017-7505: User scoped in organization with permissions for user management can manage administrators that are not assigned to any organization

05/22/2017 02:51 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>1.15.1</td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Pull request:</td>
<td><a href="https://github.com/theforeman/foreman/pull/4545">https://github.com/theforeman/foreman/pull/4545</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

It has been found that user with "_users permission who is assigned to some organization(s) can do all operations granted by these permissions on all administrator user objects. We consider admin to effectively be present in all organizations, which was the motivation for displaying them in every context.

On one hand, it make sense from technical point of view. On the other hand, it's unexpected and user that is supposed to have access to his/her organizations can edit global admin accounts including changing their passwords.

The problem seems to be present since Foreman 1.5 [1] where nesting of organizations was introduced [2]. The fix seems to be straightforward, add admin ids to the set only if User.current.admin? in Taxonomix module [3]

[2] https://github.com/theforeman/foreman/commit/1fa008a4#diff-501156756cdcbc510254e30f9e2a29daR40

Related issues:

- Related to Katello - Bug #19664: Upcoming security fix in Foreman breaks Kate... Closed 05/25/2017
- Related to foreman-tasks - Bug #19704: Upcoming security fix in Foreman break... Closed 05/30/2017
- Related to Foreman - Bug #21782: Notifications for global audience don't work Closed 11/27/2017

Associated revisions

Revision e19acaaf7 - 05/30/2017 05:40 AM - Marek Hulán
Refs #19612 - update security page

Revision af9edf10 - 06/01/2017 06:11 AM - Marek Hulán
Fixes #19612 - CVE-2017-7505 don't expose admin to taxed users

Revision 7c3d1c5c - 06/08/2017 01:26 PM - Marek Hulán
Fixes #19612 - CVE-2017-7505 don't expose admin to taxed users

(cherry picked from commit af9edf1098b8e643e16079375595e375e87ade6)

Conflicts: app/models/notification.rb

05/09/2020
History

#1 - 05/22/2017 02:52 AM - Marek Hulán
- Legacy Backlogs Release (now unused) set to 248

#2 - 05/22/2017 03:15 AM - The Foreman Bot
- Status changed from New to Ready For Testing
- Pull request https://github.com/theforeman/foreman/pull/4545 added

#3 - 05/23/2017 06:29 AM - Marek Hulán
- Subject changed from User scoped in organization with permissions for user management can manage administrators that are not assigned to any organization to CVE-2017-7505: User scoped in organization with permissions for user management can manage administrators that are not assigned to any organization

#4 - 05/25/2017 04:38 AM - Marek Hulán
- Related to Bug #19664: Upcoming security fix in Foreman breaks Katello tests added

#5 - 05/30/2017 04:45 AM - Marek Hulán
- Related to Bug #19704: Upcoming security fix in Foreman breaks KeepCurrentUser middleware added

#6 - 06/01/2017 07:01 AM - Anonymous
- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100

Applied in changeset af9edf1098b8e643e1607f9375595e375e7ade6.

#7 - 11/27/2017 01:58 PM - Marek Hulán
- Related to Bug #21782: Notifications for global audience don't work added