

## Foreman - Bug #10829

### CVE-2015-3235 - edit\_users permission allows changing of admin passwords

06/16/2015 03:27 AM - Dominic Cleal

<b>Status:</b> Closed	
<b>Priority:</b> High	
<b>Assignee:</b> Shlomi Zadok	
<b>Category:</b> Users, Roles and Permissions	
<b>Target version:</b> 1.9.0	
<b>Difficulty:</b>	<b>Fixed in Releases:</b>
<b>Triaged:</b>	<b>Found in Releases:</b>
<b>Bugzilla link:</b> 1233084	<b>Red Hat JIRA:</b>
<b>Pull request:</b> <a href="https://github.com/foreman/foreman/pull/2465">https://github.com/foreman/foreman/pull/2465</a>	
<b>Description</b>	
<p>A user with the edit_users permission (e.g. with the Manager role) is allowed to edit admin users. This allows them to change the password of the admin user's account and gain access to it.</p> <p>Tracked as CVE-2015-3235.</p>	
<b>Mitigation</b>	
<p>Change roles of users with the edit_users permission, remove the "Unlimited" flag and set a search query of "admin = false".</p>	

#### Associated revisions

##### Revision f97fbd6f - 06/16/2015 11:55 AM - Shlomi Zadok

fixes #10829 - non-admin user cannot update admin password

#### History

##### #1 - 06/16/2015 03:34 AM - Shlomi Zadok

- Assignee set to Shlomi Zadok

##### #2 - 06/16/2015 05:32 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Pull request <https://github.com/foreman/foreman/pull/2465> added

- Pull request deleted ()

##### #3 - 06/16/2015 12:01 PM - Shlomi Zadok

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset [f97fbd6f70cccd749f3bb2bece6e64d01d540561c](#).

##### #4 - 06/18/2015 04:18 AM - Ohad Levy

- Bugzilla link set to 1233084