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.

Tracked as CVE-2015-3235.

Mitigation

Change roles of users with the edit_users permission, remove the "Unlimited" flag and set a search query of "admin = false".

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/theforeman/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 97fbd6f70ccd749f3bb2bece6e6d01d540561c.

#4 - 06/18/2015 04:18 AM - Ohad Levy
- Bugzilla link set to 1233084