Foreman - Bug #2630

Users with create/edit user permissions can escalate to admin

06/07/2013 05:12 AM - Dominic Cleal

Status:	Closed		
Priority:	Urgent		
Assignee:	Marek Hulán		
Category:	Security		
Target version:	1.2.0		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

Any non-admin user with permissions to create or edit other users is able to change the admin flag, or assign roles that they themselves don't have, enabling a privilege escalation.

By default, Foreman ships with a "Site manager" role which has the edit_users permission. Any user assigned this role, or another with equivalent permissions, would be able to enable the admin flag or other roles on a user account.

This security issue has been assigned the identifier CVE-2013-2113. It affects all Foreman versions prior to 1.2.0-RC2.

Thank you to Ramon de C Valle for identifying and notifying us of this vulnerability.

Associated revisions

Revision bae665de - 06/07/2013 05:17 AM - Marek Hulán

fixes #2630 - restrict assignment of roles to those a user has (CVE-2013-2113)

Revision b52383d0 - 06/07/2013 05:18 AM - Marek Hulán

fixes #2630 - restrict assignment of roles to those a user has (CVE-2013-2113)
(cherry picked from commit bae665de387d63f93740670ec2542db90084d0eb)

Revision 7eadf32c - 06/07/2013 05:20 AM - Marek Hulán

fixes #2630 - restrict assignment of roles to those a user has (CVE-2013-2113)
(cherry picked from commit bae665de387d63f93740670ec2542db90084d0eb)

History

#1 - 06/07/2013 05:16 AM - Dominic Cleal

- Priority changed from Normal to Urgent

#2 - 06/07/2013 05:27 AM - Dominic Cleal

Patches have been committed to develop and 1.2-stable branches. Foreman 1.2.0-RC2 will contain a fix.

Foreman 1.1 stable users may apply the following patch: https://github.com/theforeman/foreman/commit/7eadf32c.patch

#3 - 06/07/2013 06:17 AM - Marek Hulán

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 7eadf32c83381aadc092cded68efff04ef20e07a.