Foreman - Bug #2631

Remote code execution in Foreman via bookmark controller name

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

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

Description

There is a code injection vulnerability in the create method of the Bookmarks controller. The create method uses the controller attribute of the newly created bookmark in an eval statement without sanitizing it.

This security issue has been assigned the identifier CVE-2013-2121. 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 ef4b97d1 - 06/07/2013 05:17 AM - Joseph Magen

fixes #2631 - fix remote code execution via controller name (CVE-2013-2121)

Revision 2f3839eb - 06/07/2013 05:19 AM - Joseph Magen

fixes #2631 - fix remote code execution via controller name (CVE-2013-2121)
(cherry picked from commit ef4b97d177c58c9532730d53dca0517bc869a0ce)

Conflicts:
app/views/common/_puppetclasses_or_envs_changed.html.erb

Revision 8920e796 - 06/07/2013 05:20 AM - Joseph Magen

fixes #2631 - fix remote code execution via controller name (CVE-2013-2121)
(cherry picked from commit ef4b97d177c58c9532730d53dca0517bc869a0ce)

History

#1 - 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/8920e796.patch

#2 - 06/07/2013 06:17 AM - Joseph Magen

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 8920e796a285201e9e0f6af0220e79d257077d7d.