Foreman - Bug #6580

CVE-2014-3531 - XSS in operating system name / description

07/11/2014 03:43 AM - Dominic Cleal

Status:	Closed		
Priority:	High		
Assignee:	Daniel Lobato Garcia		
Category:	Security		
Target version:	1.5.2		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1106417	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/1580		

Description

Reported by Jan Hutař via RHBZ:

There is a possible XSS with operating system name/description.

Version-Release number of selected component (if applicable):
Satellite-6.0.3-RHEL-6-20140605.0

How reproducible:
always

Steps to Reproduce:
1. Go to Hosts -> Operating systems -> Create new operating system
2. Fill "Name: TODO" in
- OR -
Fill some "Name" and "Description: TODO" in
3. Submit

Actual results:
In a list of operating systems unescaped string is displayed

Expected results:
HTML should be escaped

Associated revisions

Revision 98e584f5 - 07/15/2014 07:46 AM - Daniel Lobato Garcia

Fixes #6580 - XSS in operating system name/description (CVE-2014-3531)

Revision bc7e27c5 - 07/28/2014 07:28 AM - Daniel Lobato Garcia

Fixes #6580 - XSS in operating system name/description (CVE-2014-3531)

(cherry picked from commit 98e584f5a7860fb92a9916d5e5ec524372e3f8ae)

History

#1 - 07/11/2014 03:46 AM - Dominic Cleal

- Subject changed from XSS in operating system name / description to CVE-2014-3531 - XSS in operating system name / description

#2 - 07/11/2014 04:09 AM - Daniel Lobato Garcia

- Status changed from Assigned to Ready For Testing

- Pull request https://github.com/theforeman/foreman/pull/1580 added

- Pull request deleted ()

#3 - 07/15/2014 08:01 AM - Daniel Lobato Garcia

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 98e584f5a7860fb92a9916d5e5ec524372e3f8ae.

#4 - 07/15/2014 08:47 AM - The Foreman Bot

- Status changed from Closed to Ready For Testing

#5 - 07/21/2014 04:05 AM - Dominic Cleal

- Status changed from Ready For Testing to Closed

#6 - 07/28/2014 07:46 AM - Dominic Cleal

Fix released today in Foreman 1.5.2. Details posted on http://theforeman.org/security.html#2014-3531.