Foreman - Bug #6580
CVE-2014-3531 - XSS in operating system name / description

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

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>High</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Daniel Lobato Garcia</td>
</tr>
<tr>
<td>Category:</td>
<td>Security</td>
</tr>
<tr>
<td>Target version:</td>
<td>1.5.2</td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Pull request:</td>
<td><a href="https://github.com/theforeman/foreman/pull/1580">https://github.com/theforeman/foreman/pull/1580</a></td>
</tr>
<tr>
<td>Triaged:</td>
<td></td>
</tr>
<tr>
<td>Bugzilla link:</td>
<td>1106417</td>
</tr>
<tr>
<td>Fixed in Releases:</td>
<td></td>
</tr>
<tr>
<td>Found in Releases:</td>
<td></td>
</tr>
</tbody>
</table>

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: T<o>D" in
   - OR -
3. Fill some "Name" and "Description: T<o>D" 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

03/15/2020
- 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 98e584f5a7860fb92a991ed55e524372e3f8ae.

#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.