Foreman - Bug #20963

CVE-2017-7535: stored XSS in the manage organization page

09/17/2017 06:31 AM - Tomer Brisker

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Low</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Tomer Brisker</td>
</tr>
<tr>
<td>Category:</td>
<td>Security</td>
</tr>
<tr>
<td>Target version:</td>
<td>1.16.0</td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Pull request:</td>
<td><a href="https://github.com/theforeman/foreman/pull/4851">https://github.com/theforeman/foreman/pull/4851</a></td>
</tr>
</tbody>
</table>

Description

Attempting to assign all hosts to an organization or location that contains HTML does not properly escape the html in the toast notification informing of success. Setting priority to low since exploiting this requires a user to actively assign hosts to an organization that contains html in its name which is visible to the user prior to taking action.

Associated revisions

Revision b8db2f93 - 09/19/2017 02:46 AM - Tomer Brisker
Fixes #20963 - CVE-2017-7535 prevent XSS on org/loc host assign

Revision 08aea206 - 09/19/2017 06:48 AM - Tomer Brisker
Fixes #20963 - CVE-2017-7535 prevent XSS on org/loc host assign
(cherry picked from commit b8db2f931208992d6bcff44a2d20101637f6c232)

History

#1 - 09/17/2017 07:21 AM - The Foreman Bot
- Status changed from New to Ready For Testing
- Pull request https://github.com/theforeman/foreman/pull/4851 added

#2 - 09/18/2017 10:14 AM - Daniel Lobato Garcia
- Legacy Backlogs Release (now unused) set to 240

#3 - 09/19/2017 03:01 AM - Anonymous
- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100

Applied in changeset b8db2f931208992d6bcff44a2d20101637f6c232.