Foreman - Bug #16024
Foreman form helpers do not escape JS when rendering label
08/09/2016 08:55 AM - Marek Hulán

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Marek Hulán</td>
</tr>
<tr>
<td>Category:</td>
<td>Security</td>
</tr>
<tr>
<td>Target version:</td>
<td>1.12.2</td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Pull request:</td>
<td><a href="https://github.com/theforeman/foreman/pull/3715">https://github.com/theforeman/foreman/pull/3715</a></td>
</tr>
<tr>
<td>Triaged:</td>
<td>Fix in Releases:</td>
</tr>
<tr>
<td>Bugzilla link:</td>
<td>Found in Releases: 1.6.0</td>
</tr>
</tbody>
</table>

**Description**
The issue was introduced in Foreman 1.6. There's only one dynamic :label => in Foreman that uses MailNotification name which we don't allow users to modify so there's no vulnerable code in Foreman. But remote execution plugin that rely on this label to be escaped. Setting to 1.12.2, feel free to reset. For REX this is pretty important though.

**Related issues:**
Related to Foreman Remote Execution - Bug #16019: CVE-2016-6319 - Persistent ... Resolved 08/09/2016

**Associated revisions**
Revision 0f35fe14 - 08/10/2016 06:26 AM - Marek Hulán
Fixes #16024 - escape labels of form fields

Revision 15a6c9b1 - 08/23/2016 10:49 AM - Marek Hulán
Fixes #16024 - escape labels of form fields
(cherry picked from commit 0f35fe14acf0d0d3b55e9337bc5e2b9640f2372)

**History**

#1 - 08/09/2016 08:56 AM - The Foreman Bot
- Status changed from New to Ready For Testing
- Pull request https://github.com/theforeman/foreman/pull/3715 added

#2 - 08/09/2016 08:57 AM - Marek Hulán
- Category changed from Web Interface to Security

#3 - 08/09/2016 08:57 AM - Marek Hulán
- Related to Bug #16019: CVE-2016-6319 - Persistent XSS in job invocation form triggered by unescaped user input name added

#4 - 08/10/2016 07:01 AM - Marek Hulán
- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100

Applied in changeset 0f35fe14acf0d0d3b55e9337bc5e2b9640f2372.