Foreman - Bug #24807
CVE-2018-16861 - toast notification sends strings through as HTML
09/04/2018 12:27 PM - Chris Duryee

<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>Avi Sharvit</td>
</tr>
<tr>
<td>Category</td>
<td>Security</td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
</tr>
<tr>
<td>Difficulty</td>
<td></td>
</tr>
<tr>
<td>Triaged</td>
<td>No</td>
</tr>
<tr>
<td>Bugzilla link</td>
<td>1652785</td>
</tr>
<tr>
<td>Fixed in Releases:</td>
<td>1.18.3, 1.19.1, 1.20.0</td>
</tr>
<tr>
<td>Found in Releases:</td>
<td>1.16.0, 1.16.0-RC1, 1.16.0-RC2, 1.16.1, 1.16.2, 1.17.0, 1.17.0-RC1, 1.17.0-RC2, 1.17.1, 1.17.2, 1.17.3, 1.17.4, 1.18.0, 1.18.0-RC1, 1.18.0-RC2, 1.18.0-RC3, 1.18.1, 1.18.2, 1.19.0, 1.19.0-RC1, 1.19.0-RC2, 1.19.0-RC3</td>
</tr>
</tbody>
</table>

Description
If you call `Notification.setErrorMessage()` with a string that contains `<` and `>`, the string will get sent through to the browser and the browser will attempt to render it as HTML.

For example, it's possible to get Pulp to raise an error message like "The configuration parameter <foo> is not valid". This will display in the browser as "The configuration parameter is not valid".

It would be better if the notification escaped these strings so the "<>" is not lost.

Related issues:
Related to Foreman - Bug #25230: compute resource test connection is html inc... Closed

Associated revisions
Revision 744091c5 - 09/06/2018 01:06 PM - Avi Sharvit
Fixes #24807 - unsafe html in toast notification

toast notification sends strings through as HTML

History
#1 - 09/04/2018 02:17 PM - John Mitsch
I think this is related to the dangerouslySetInnerHTML prop here
https://github.com/theforeman/foreman/blob/develop/webpack/assets/javascripts/react_app/components/common/Alert/AlertBody.js#L13

#2 - 09/05/2018 01:48 PM - Tomer Brisker
- Priority changed from Normal to High
- Assignee set to Avi Sharvit
- Category set to Security

#3 - 09/05/2018 02:08 PM - Tomer Brisker
- Found in Releases 1.16.0, 1.16.0-RC1, 1.16.0-RC2, 1.16.1, 1.16.2, 1.17.0, 1.17.0-RC1, 1.17.0-RC2, 1.17.1, 1.17.2, 1.17.3, 1.17.4, 1.18.0, 1.18.0-RC1, 1.18.0-RC2, 1.18.0-RC3, 1.18.1, 1.18.2, 1.19.0, 1.19.0-RC1, 1.19.0-RC2, 1.19.0-RC3 added
This was introduced in [https://github.com/theforeman/foreman/commit/68cd4bba826df1e155445b1f10a7fc2cb186c9d82](https://github.com/theforeman/foreman/commit/68cd4bba826df1e155445b1f10a7fc2cb186c9d82) which is in 1.16.0 or newer.

On the server side, when using the foreman core functions for toast notifications, the messages are escaped: [https://github.com/theforeman/foreman/blob/develop/app/controllers/concerns/foreman/controller/flash.rb#L67](https://github.com/theforeman/foreman/blob/develop/app/controllers/concerns/foreman/controller/flash.rb#L67) therefor this could only be exploited from creating a toast notification in a different manner.

#4 - 09/05/2018 03:33 PM - The Foreman Bot
- Status changed from New to Ready For Testing
- Pull request [https://github.com/theforeman/foreman/pull/6041](https://github.com/theforeman/foreman/pull/6041) added

#5 - 09/06/2018 01:10 PM - Tomer Brisker
- Fixed in Releases 1.19.1, 1.20.0 added

Foreman core helpers already escape messages before passing them on to the notifications, and therefore this isn't a significant risk of XSS here, but we fixed it just to be on the safe side.

#6 - 09/06/2018 02:01 PM - Avi Sharvit
- Status changed from Ready For Testing to Closed

Applied in changeset [744091c54261b892306b010e8dc0ea8d593515fa](https://github.com/theforeman/foreman/pull/6041).

#7 - 09/12/2018 09:31 AM - The Foreman Bot
- Pull request [https://github.com/theforeman/foreman/pull/6060](https://github.com/theforeman/foreman/pull/6060) added

#8 - 10/04/2018 02:17 PM - Tomer Brisker
- Fixed in Releases 1.18.3 added

#9 - 10/18/2018 12:43 PM - Ohad Levy
- Related to Bug #25230: compute resource test connection is html incorrectly escaped added

#10 - 11/23/2018 06:18 AM - Tomer Brisker
- Bugzilla link set to 1652785

#11 - 11/25/2018 08:22 AM - Tomer Brisker
- Subject changed from toast notification sends strings through as HTML to CVE-2018-16861 - toast notification sends strings through as HTML