## Foreman - Bug #16022

### CVE-2016-6320 - Network interface device identifiers may contain stored XSS on host form

08/09/2016 08:04 AM - Dominic Cleal

<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>Tomer Brisker</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/3714">https://github.com/theforeman/foreman/pull/3714</a></td>
</tr>
<tr>
<td>Triaged:</td>
<td></td>
</tr>
<tr>
<td>Bugzilla link:</td>
<td>1421803</td>
</tr>
<tr>
<td>Fixed in Releases:</td>
<td></td>
</tr>
<tr>
<td>Found in Releases:</td>
<td></td>
</tr>
</tbody>
</table>

### Description

Network interface identifiers stored for hosts may contain HTML or JavaScript that allows a stored XSS (cross-site scripting) vulnerability when later viewing the host edit form.

This issue was reported by Sanket Jagtap.

CVE identifier will be assigned.

### Associated revisions

**Revision 53081ea1 - 08/10/2016 03:23 AM - Tomer Brisker**

Fixes #16022 - Prevent stored XSS in host interface form

The host interface form may contain a stored XSS in the identifier field allowing a user allowed to edit a host's interfaces to cause code execution by another user viewing that host's edit form.

**Revision 2ab766fa - 08/23/2016 10:49 AM - Tomer Brisker**

Fixes #16022 - Prevent stored XSS in host interface form

The host interface form may contain a stored XSS in the identifier field allowing a user allowed to edit a host's interfaces to cause code execution by another user viewing that host's edit form.

(cherry picked from commit 53081ea14b30d66f0d67b62fe950a2c1463225f5)

### History

**#1 - 08/09/2016 08:13 AM - The Foreman Bot**

- Status changed from New to Ready For Testing
- Assignee set to Tomer Brisker
- Pull request https://github.com/theforeman/foreman/pull/3714 added

**#2 - 08/09/2016 10:09 AM - Tomer Brisker**

- Target version set to 1.7.1
#3 - 08/10/2016 04:02 AM - Anonymous
- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100

Applied in changeset 53081ea14b30d66f0d67b62fe950a2c1463225f5.

#4 - 08/10/2016 04:49 AM - Dominic Cleal
- Subject changed from Network interface device identifiers may contain stored XSS on host form to CVE-2016-6320 - Network interface device identifiers may contain stored XSS on host form

#5 - 08/23/2016 09:59 AM - Daniel Lobato Garcia
- Target version changed from 1.7.1 to 1.6.2

#6 - 08/23/2016 11:06 AM - Daniel Lobato Garcia
- Target version changed from 1.6.2 to 1.7.1

#7 - 03/15/2017 03:32 PM - Ohad Levy
- Bugzilla link set to 1421803