The host YAML view (preview of YAML data for Puppet) is vulnerable to cross-site scripting attacks, when data relating to the host (such as parameters) contains HTML content.

1. Edit a host, add a parameter with HTML as its name or value
2. View the host, click the YAML button
Changes in Foreman:

#4 - 06/11/2014 03:25 PM - Dominic Cleal
- Subject changed from EMBARGOED: XSS in host YAML view to EMBARGOED: CVE-2014-3492 - XSS in host YAML view

#5 - 06/11/2014 05:46 PM - Dominic Cleal
- Status changed from Ready For Testing to Pending

ACK, thanks Lukas!

#6 - 06/11/2014 06:23 PM - Dominic Cleal
- Target version changed from 1.8.2 to 1.8.1

#7 - 06/13/2014 12:46 PM - Dominic Cleal
- Legacy Backlogs Release (now unused) changed from 16 to 19

#8 - 06/18/2014 08:01 AM - Dominic Cleal
- Subject changed from EMBARGOED: CVE-2014-3492 - XSS in host YAML view to CVE-2014-3492 - XSS in host YAML view
- Description updated
- Private changed from Yes to No

#9 - 06/18/2014 08:31 AM - Lukas Zapletal
- Status changed from Pending to Closed
- % Done changed from 0 to 100

Applied in changeset d40f5409ac36e1eab7b8a5ccf3d91cc6db90ce70.

#10 - 06/18/2014 09:09 AM - Dominic Cleal
Fixes committed to 1.4-stable, 1.5-stable and develop.

Foreman 1.4.5 and 1.5.1 releases will be made today with the fix.

Files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001-fixes-6149-fixed-XSS-in-host-YAML-view.patch</td>
<td>886 Bytes</td>
<td>06/11/2014</td>
<td>Lukas Zapletal</td>
</tr>
</tbody>
</table>