Foreman - Bug #6149
CVE-2014-3492 - XSS in host YAML view
06/10/2014 08:46 PM - Dominic Cleal

Status: Closed
Priority: Urgent
Assignee: Lukas Zapletal
Category: Security
Target version: 1.4.5

Description
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

Associated revisions
Revision d40f5409 - 06/18/2014 08:02 AM - Lukas Zapletal
fixes #6149 - fixed XSS in host YAML view (CVE-2014-3492)

Revision d7546f37 - 06/18/2014 08:03 AM - Lukas Zapletal
fixes #6149 - fixed XSS in host YAML view (CVE-2014-3492)
(cherry picked from commit d40f5409ac36c1eb7b8a5ccf3d91cc6db90ce70)

Revision b6007279 - 06/18/2014 08:04 AM - Lukas Zapletal
fixes #6149 - fixed XSS in host YAML view (CVE-2014-3492)

History
#1 - 06/11/2014 01:30 PM - Lukas Zapletal
- Status changed from New to Assigned
- Assignee set to Lukas Zapletal

Reproduced, working on a fix.

#2 - 06/11/2014 02:16 PM - Lukas Zapletal
- File 0001-fixes-6149-fixed-XSS-in-host-YAML-view.patch added

Attached is a fix that escapes HTML.

#3 - 06/11/2014 02:19 PM - Lukas Zapletal
- Status changed from Assigned to Ready For Testing

Please review.
#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 d40f5409ac36c1eab7b8a5ccf3d91cc6db90ce70.

#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
0001-fixes-6149-fixed-XSS-in-host-YAML-view.patch 886 Bytes 06/11/2014  Lukas Zapletal