Sending a fact name or value containing HTML can lead to a stored XSS in the following pages:

- Facts page - When opening a chart for a fact that has HTML in it's name or as one of the values.
- Trends page - A trend containing a value that includes HTML in it.
- Statistics page - Fact values that are aggregated on the page such as manufacturer and contain HTML.

This issue has been reported by Roman Mueller.

**Related issues:**
Related to Foreman - Bug #24834: Fact names and values are not displayed prop...

**Associated revisions**

Revision 81e40e3a - 11/05/2017 02:55 PM - Tomer Brisker
Fixes #21519 - Prevent stored XSS on fact charts

**History**

#1 - 10/31/2017 05:07 PM - Tomer Brisker
- Legacy Backlogs Release (now unused) set to 240

Setting for 1.16 for now, will possibly do another 1.15 release if needed.

#2 - 10/31/2017 05:28 PM - Tomer Brisker
- Description updated

#3 - 10/31/2017 05:36 PM - The Foreman Bot
- Status changed from Assigned to Ready For Testing
- Pull request https://github.com/theforeman/foreman/pull/4967 added

#4 - 11/05/2017 09:53 AM - Tomer Brisker
- Subject changed from Stored XSS in fact name or value to CVE-2017-15100: Stored XSS in fact name or value

#5 - 11/05/2017 03:02 PM - Anonymous
- % Done changed from 0 to 100
- Status changed from Ready For Testing to Closed

Applied in changeset 81e40e3a14a90c11c4193bebc7eeeb79c2cfd9b1.
#6 - 03/19/2018 08:31 PM - Bryan Kearney
- Bugzilla link set to 1509442

#7 - 09/06/2018 11:32 AM - Marek Hulán
- Related to Bug #24834: Fact names and values are not displayed properly added