When creating an organization or location, if the name contains HTML then the second step of the wizard (/organizations/id/step2) will render the HTML.

This occurs in the alert box stating that "Assigning hosts to ... will also update ... to include all the resources that the selected hosts are currently using."

This may permit a stored XSS attack if an organization with HTML in its name was added, then a user was directed to the specific URL of the wizard. However there are no direct links back to the wizard, so ordinarily this would only affect the user who created the org/location.

Affects Foreman 1.1 and higher.

Reported by Sanket Jagtap to foreman-security@googlegroups.com.

Revision 5a573456 - 11/08/2016 07:41 AM - Tomer Brisker

Fixes #17195 - CVE-2016-8634 escape html in alert text

The alert helper used to mark the alert text as html_safe by default. However, in some cases it may be possible for a user to enter custom text into the alert message leading to a possible XSS vulnerability. This patch changes this so that text is escaped unless explicitly marked as html_safe in the code.

History

#1 - 11/03/2016 09:21 AM - Dominic Cleal
- Subject changed from Organization/location wizard may run stored XSS through alert to CVE-2016-8634 - Organization/location wizard may run stored XSS through alert

#2 - 11/06/2016 07:39 AM - Tomer Brisker
- Status changed from New to Assigned
- Assignee set to Tomer Brisker

#3 - 11/06/2016 07:59 AM - The Foreman Bot
- Status changed from Assigned to Ready For Testing
- Pull request https://github.com/theforeman/foreman/pull/3996 added

#4 - 11/08/2016 08:01 AM - Anonymous

- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100

Applied in changeset 5a573456b5ecb3ba0d24e057722704f9afeda8f7.