

## Foreman - Bug #11859

### CVE-2015-5282 - Parameter hide/show checkbox allows stored XSS during textbox change

09/17/2015 04:01 AM - Dominic Cleal

<b>Status:</b> Closed	
<b>Priority:</b> Normal	
<b>Assignee:</b> Shlomi Zadok	
<b>Category:</b> Security	
<b>Target version:</b> 1.10.0	
<b>Difficulty:</b>	<b>Fixed in Releases:</b>
<b>Triaged:</b>	<b>Found in Releases:</b>
<b>Bugzilla link:</b> 1268995	<b>Red Hat JIRA:</b>
<b>Pull request:</b> <a href="https://github.com/foreman/foreman/pull/2736">https://github.com/foreman/foreman/pull/2736</a>	
<b>Description</b>	
<p>We allow storage of key/value parameters globally or assigned to various objects, and using a tickbox in the UI the values can be hidden to mask them from casual viewing. The tickbox that hides/shows the value fails to handle HTML properly and so is vulnerable to an XSS issue where HTML can be stored in a parameter, and executed by another user if they later tick the hide/show box.</p> <p>An example on the global parameters form is:</p> <pre>"&gt;&amp;lt;script&amp;gt;alert("hi")&amp;lt;/script&amp;gt;&amp;lt;b c="&amp;gt;</pre> <p>Store this in a parameter value, reload the page and click the "Hidden value" checkbox and the JavaScript will execute. The reverse is probably possible too.</p>	

#### Associated revisions

##### Revision 4f3555b2 - 09/21/2015 05:38 AM - Shlomi Zadok

Fixes #11859 - handle HTML in parameters safely when hiding values (CVE-2015-5282)

#### History

##### #1 - 09/17/2015 05:50 PM - The Foreman Bot

- Status changed from New to Ready For Testing
- Pull request <https://github.com/foreman/foreman/pull/2736> added
- Pull request deleted ()

##### #2 - 09/18/2015 03:03 AM - Dominic Cleal

- Subject changed from Parameter hide/show checkbox allows XSS during textbox change to CVE-2015-5282 - Parameter hide/show checkbox allows stored XSS during textbox change
- Description updated

##### #3 - 09/21/2015 05:39 AM - Dominic Cleal

- Assignee set to Shlomi Zadok

##### #4 - 09/21/2015 06:01 AM - Shlomi Zadok

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

Applied in changeset [4f3555b217be8723e8045f9816d147b5f684ec57](#).

##### #5 - 10/15/2015 09:36 AM - Bryan Kearney

- Bugzilla link set to 1268995