Foreman - Bug #5471

CVE-2014-0208 - Stored XSS inside search auto-complete key names via parameters

04/28/2014 12:36 PM - Dominic Cleal

Status:	Closed		
Priority:	High		
Assignee:	Amos Benari		
Category:	Security		
Target version:	1.4.4		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1088315	**Red Hat JIRA:**	
Pull request:			

Description

Reported by Jan Hutař of Red Hat.

Description of problem:
There is a possible XSS: Configure -> Global parameters - key name with HTML evaluated when auto-completing

How reproducible:
always

Steps to Reproduce:
1. In webUI go to Configure -> Global parameters -> New Parameter
2. Fill in this:
Name: test<script>alert('HI')</script>
Value: something
Click "Submit" to create the parameter
3. Note that parameter name is correctly escaped in the parameters list
4. In the search bar above the table with parameters type "name = "
and wait for auto-complete function to display you recommendations

Actual results:
Once the recommendations are displayed, JavaScript alert window appears (script gets executed)

Expected results:
Stuff should be escaped in the suggested list.

Additional info:
Same happens for "value" when you type "value = " into the search box.

Associated revisions

Revision ee672544 - 05/08/2014 01:42 PM - Amos Benari

fixes #5471 html escape auto-completer values (CVE-2014-0208)

Revision 25d9019c - 05/08/2014 01:47 PM - Amos Benari

fixes #5471 html escape auto-completer values (CVE-2014-0208)

(cherry picked from commit ee672544f1ad5990ca0e39acd86f83cbbe06ebe9)

Revision 5d3f892c - 05/08/2014 01:47 PM - Amos Benari

fixes #5471 html escape auto-completer values (CVE-2014-0208)

(cherry picked from commit ee672544f1ad5990ca0e39acd86f83cbbe06ebe9)

History

#1 - 04/29/2014 01:29 PM - Dominic Cleal

- Status changed from New to Ready For Testing

- Assignee set to Amos Benari

- translation missing: en.field_release set to 17

#2 - 05/06/2014 08:33 AM - Dominic Cleal

- Subject changed from Stored XSS inside search auto-complete key names via parameters to CVE-2014-0208 - Stored XSS inside search auto-complete key names via parameters

#3 - 05/07/2014 11:06 AM - Dominic Cleal

- File 0001-fixes-5471-html-escape-auto-completer-values.patch added

- Status changed from Ready For Testing to Pending

Attaching patch from Amos against develop.

#4 - 05/08/2014 01:44 PM - Dominic Cleal

- Private changed from Yes to No

#5 - 05/08/2014 02:31 PM - Amos Benari

- Status changed from Pending to Closed

- % Done changed from 0 to 100

Applied in changeset ee672544f1ad5990ca0e39acd86f83cbbe06ebe9.

Files

0001-fixes-5471-html-escape-auto-completer-values.patch	1.53 KB	05/07/2014	Dominic Cleal