Foreman - Bug #4456

CVE-2014-0089 - Stored Cross Site Scripting (XSS) on 500 error page

02/26/2014 08:17 AM - Dominic Cleal

Status:	Closed		
Priority:	Urgent		
Assignee:	Joseph Magen		
Category:	Security		
Target version:	1.4.2		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.4.0
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

Description
Any user who has a privilege to add bookmarks could exploit the cross site scripting vulnerability to expose other users' personal data by storing malicious scripts when adding bookmark. As the script is permanently stored, every time others access /bookmarks to view the bookmarks, they will be affected.

Severity: High

Affected URLs
http://$foreman/bookmarks

Steps
Add a bookmark with some script code(e.g. <script>alert('xss')</script>) set as its bookmark name
Access /bookmarks to view bookmarks

Result
The script will be executed.

Remedy advice
User inputs such as special characters must be validated, filtered or encoded before being returned as part of the HTML code of a page.

Reference
CWE-931 - http://cwe.mitre.org/data/definitions/931.html

Affects
Foreman 1.4.0 and higher. Foreman 1.3 and older are unaffected, they correctly escape the message.

Related issues:

Related to Foreman - Bug #4519: Renaming host with / in name causes "No route...	**Closed**	**03/03/2014**

Associated revisions

Revision 69e46d6d - 03/24/2014 08:32 AM - Joseph Magen

fixes #4456 - XSS on 500 error page and bookmark name causing render error (CVE-2014-0089)

Revision 83169c12 - 03/24/2014 08:57 AM - Joseph Magen

fixes #4456 - XSS on 500 error page and bookmark name causing render error (CVE-2014-0089)

(cherry picked from commit 69e46d6d6eb230f3aa4236838999284dfffccb6e)

History

#1 - 02/26/2014 10:45 AM - Dominic Cleal

- Subject changed from Bookmark names are vulnerable to XSS to CVE-2014-0089 - Bookmark names are vulnerable to XSS

- Description updated

#2 - 02/26/2014 04:29 PM - Dominic Cleal

- File 0001-fixes-bookmark-error.patch added

Unreviewed v1 patch from Joseph.

#3 - 02/26/2014 06:33 PM - Greg Sutcliffe

I can't replicate this. A bookmark with the example code as name displays correctly on my bookmarks page, performs the search if selected on the Hosts page, and does not trigger the script when loaded - this is true both for admin and a normal user (with view_bookmarks, as tested with Marek's new rbac pr applied). Using Firefox 27.0.

The DB seems to show that no character conversion has occurred during save:

```
sqlite> select * from bookmarks;
7|<script>alert('xss')</script>|foo|hosts|t|1|User
```

The HTML of the page confirms it's displaying them safely:

```
<td><a class=" disabled" disabled="disabled" href="#" onclick="; return false;">&lt;script&gt;alert(&#x27;xss&
#x27;)&lt;/script&gt;</a></td>
```

Just for fun I applied the attached patch anyway, and confirmed the all same behaviour and results, so the patch doesn't change anything, as far as I can tell.

#4 - 02/27/2014 07:43 AM - Ohad Levy

the issue is really with the exception 500 page, as the exception is treated as html safe.

every other place that you can generate an exception based on input will have this issue.

@Greg Sutcliffe, I had no problem to replicate this, ping me if you like to go over it togther

#5 - 02/27/2014 07:45 AM - Joseph Magen

Greg, you must start the rails server in production mode to see the error.

#6 - 03/03/2014 11:25 AM - Dominic Cleal

- Subject changed from CVE-2014-0089 - Bookmark names are vulnerable to XSS to CVE-2014-0089 - Stored Cross Site Scripting (XSS) on 500 error page

To clarify, as Ohad said, this is an issue on the 500 error page. The bookmark page is failing to render and find an appropriate route for the bookmark containing the script tag, triggering a 500 error (which is a minor/partial DoS in itself, but not CVE-worthy) and then the 500 error page is rendering the error without HTML escaping.

#7 - 03/03/2014 11:26 AM - Dominic Cleal

- Description updated

Affects Foreman 1.4.0 and higher. Foreman 1.3 and older are unaffected, they correctly escape the message.

#8 - 03/03/2014 12:08 PM - Dominic Cleal

- Related to Bug #4519: Renaming host with / in name causes "No route matches" error added

#9 - 03/03/2014 01:01 PM - Dominic Cleal

- Target version changed from 1.9.1 to 1.9.0

#10 - 03/04/2014 02:03 PM - Dominic Cleal

- Due date set to 03/18/2014

#11 - 03/04/2014 02:12 PM - Dominic Cleal

- Status changed from Assigned to Pending

ACK, patch v1 is good.

#13 - 03/24/2014 08:56 AM - Dominic Cleal

- Private changed from Yes to No

#14 - 03/24/2014 09:31 AM - Joseph Magen

- Status changed from Pending to Closed

- % Done changed from 0 to 100

Applied in changeset 69e46d6d6eb230f3aa4236838999284dfffccb6e.

#15 - 03/25/2014 09:43 AM - Dominic Cleal

- Description updated

Files

0001-fixes-bookmark-error.patch	2.01 KB	02/26/2014	Dominic Cleal