Foreman - Bug #5881

CVE-2014-3491 - XSS from create/update/destroy notification boxes

05/22/2014 02:40 PM - Dominic Cleal

Status:	Closed		
Priority:	High		
Assignee:	Joseph Magen		
Category:	Security		
Target version:	1.4.5		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1100313	**Red Hat JIRA:**	
Pull request:			

Description

possible XSS: Configure -> Host groups - key name with HTML evaluated when submitted

How reproducible:
always

Steps to Reproduce:
1. In webUI go to Configure -> Host groups -> New Host groups
2. Fill in this:
Name: test<script>alert('HI')</script>

```
Click "Submit" to create the hostgroup
3. Note that parameter name is correctly escaped in the parameters list
```

Actual results:
Once the hostgroup is SUBMITED, JavaScript alert window appears (script gets executed)

Expected results:
Submit button should not execute javascript

Related issues:

Related to Foreman - Bug #6351: <br /> seen in UI errors when multiple errors...	**Duplicate**	**06/24/2014**
Related to Foreman - Bug #6402: Using "run puppet" feature fails: undefined m...	**Closed**	**06/26/2014**
Related to Foreman - Bug #6903: "<br/>" in text when receiving error while de...	**Closed**	**08/04/2014**

Associated revisions

Revision 983075c0 - 06/18/2014 08:02 AM - Joseph Magen

fixes #5881 - XSS from create/update/destroy notification boxes (CVE-2014-3491)

Revision dae1ac11 - 06/18/2014 08:03 AM - Joseph Magen

fixes #5881 - XSS from create/update/destroy notification boxes (CVE-2014-3491)

(cherry picked from commit 983075c0c0e95c0d4715591325e88c90c7f09d71)

Revision 3d7c94c9 - 06/18/2014 08:03 AM - Joseph Magen

fixes #5881 - XSS from create/update/destroy notification boxes (CVE-2014-3491)

Conflicts:
app/controllers/concerns/foreman/controller/taxonomies_controller.rb
app/controllers/hostgroups_controller.rb
app/controllers/roles_controller.rb

History

#1 - 05/22/2014 02:42 PM - Dominic Cleal

- Subject changed from XSS from create/update/destroy notification boxes to EMBARGOED: XSS from create/update/destroy notification boxes

#2 - 05/22/2014 02:44 PM - Dominic Cleal

This appears to be coming from the popup notifications in the UI that appear when creating/updating/deleting resources. I suppose one user could create a resource with such a name and then another user could try editing or deleting it to execute the script, but when creating, a user is only going to be able to attach themselves.

The host group name is also formatted strangely in the host groups list, may be worth checking out at the same time.

(I've also seen this when deleting config groups and templates, it's a problem generally with the process_success type notifications.)

#3 - 05/27/2014 01:41 PM - Joseph Magen

- Status changed from New to Assigned

Rails automatic escapes/sanitizes text strings when saving to the db, so this is the reason of the "strange formatting"

I emailed patch.

#4 - 05/27/2014 01:43 PM - Dominic Cleal

Please just attach the patch for review here, thanks.

#5 - 06/10/2014 04:24 PM - Dominic Cleal

- File 0001-fixes-5881-XSS-from-create-update-destroy-notificati.patch added

- Assignee set to Joseph Magen

Attached is the v1 patch.

Works well, though could we escape the HTML rather than sanitizing it? Just so the actual name fully shows up.

I looked into the index name display, it's just a bug in the ancestry_helper, pretty sure it's harmless. I'll file another bug once this is unembargoed.

#6 - 06/10/2014 04:25 PM - Dominic Cleal

- translation missing: en.field_release set to 16

#7 - 06/11/2014 01:22 PM - Joseph Magen

- File 0002-fixes-5881-XSS-from-create-update-destroy-notificati.patch added

- Status changed from Assigned to Ready For Testing

new patch attached that uses CGI::escapeHTML rather than ActionController::Base.helpers.sanitize

#8 - 06/11/2014 03:24 PM - Dominic Cleal

- Subject changed from EMBARGOED: XSS from create/update/destroy notification boxes to EMBARGOED: CVE-2014-3491 - XSS from create/update/destroy notification boxes

#9 - 06/11/2014 05:20 PM - Dominic Cleal

- Status changed from Ready For Testing to Pending

ACK, thanks Joseph!

#10 - 06/11/2014 06:22 PM - Dominic Cleal

- Target version changed from 1.8.2 to 1.8.1

#11 - 06/13/2014 12:46 PM - Dominic Cleal

- translation missing: en.field_release changed from 16 to 19

#12 - 06/17/2014 04:04 PM - Dominic Cleal

- File 0001-fixes-5881-XSS-from-create-update-destroy-notificati.patch added

- File 0001-fixes-5881-XSS-from-create-update-destroy-notificati.patch added

Updated patch to fix tests, backported to 1.4-stable.

#13 - 06/18/2014 08:01 AM - Dominic Cleal

- Subject changed from EMBARGOED: CVE-2014-3491 - XSS from create/update/destroy notification boxes to CVE-2014-3491 - XSS from create/update/destroy notification boxes

- Private changed from Yes to No

#14 - 06/18/2014 08:31 AM - Joseph Magen

- Status changed from Pending to Closed

- % Done changed from 0 to 100

Applied in changeset 983075c0c0e95c0d4715591325e88c90c7f09d71.

#15 - 06/18/2014 09:08 AM - Dominic Cleal

Fixes committed to 1.4-stable, 1.5-stable and develop.

Foreman 1.4.5 and 1.5.1 releases will be made today with the fix.

#16 - 06/24/2014 08:16 AM - Dominic Cleal

- Related to Bug #6351: <br /> seen in UI errors when multiple errors exist on a resource added

#17 - 06/26/2014 04:04 PM - Dominic Cleal

- Related to Bug #6402: Using "run puppet" feature fails: undefined method `gsub' for #<Array ...> added

#18 - 08/04/2014 06:12 AM - Dominic Cleal

- Related to Bug #6903: "<br/>" in text when receiving error while deleting multiple hosts added

Files

0001-fixes-5881-XSS-from-create-update-destroy-notificati.patch	3.8 KB	06/10/2014	Dominic Cleal
0002-fixes-5881-XSS-from-create-update-destroy-notificati.patch	3.71 KB	06/11/2014	Joseph Magen
0001-fixes-5881-XSS-from-create-update-destroy-notificati.patch	4.84 KB	06/17/2014	Dominic Cleal
0001-fixes-5881-XSS-from-create-update-destroy-notificati.patch	3.38 KB	06/17/2014	Dominic Cleal