Foreman - Bug #12611

CVE-2015-7518 - Smart class parameters/variables shown on host edit allows stored XSS in description

11/26/2015 05:15 AM - Dominic Cleal

Status:	Closed		
Priority:	Normal		
Assignee:	Tomer Brisker		
Category:	Security		
Target version:	1.10.0		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1297040	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/2936		

Description

Reported by Tomer Brisker to foreman-security:

> I have discovered a stored XSS vulnerability in the host and hostgroup edit forms caused by smart class parameters and smart variables.
>
> These forms display a popover that shows additional info about any of the parameters that can be overridden. The popover is rendered with HTML but contains values that can be input by a user - the parameter description, and in develop branch also the inherited value.
>
> Effectively, any user who can edit parameters can input arbitrary HTML or JS into the description field or the default value, which will be executed once the popover is triggered by any other user.

This affects all versions of Foreman.

CVE identifier is CVE-2015-7518.

Related issues:

Related to Foreman - Feature #7163: In host's edit page, show the source for ...	**Closed**	**08/20/2014**
Related to Foreman - Feature #15495: URL's in parameter description	**New**	**06/22/2016**

Associated revisions

Revision 32468bce - 12/09/2015 08:54 AM - Tomer Brisker

Fixes #12611 - CVE-2015-7518 prevent XSS on host edit form

The host edit forms allowed stored XSS attacks by storing html content
in smart class parameter and smart variable description or inherited
values, which is then passed unescaped to an html-allowing popover.
This patch makes sure these user-controlled strings are correctly
escaped before being inserted into the popover.

Revision f5576998 - 12/11/2015 01:22 PM - Tomer Brisker

Fixes #12611 - CVE-2015-7518 prevent XSS on host edit form

The host edit forms allowed stored XSS attacks by storing html content
in smart class parameter and smart variable description or inherited
values, which is then passed unescaped to an html-allowing popover.
This patch makes sure these user-controlled strings are correctly
escaped before being inserted into the popover.

(cherry picked from commit 32468bce938067b1bbde1c2025771b5b83ce88ec)

History

#1 - 11/26/2015 05:52 AM - Dominic Cleal

- Subject changed from Smart class parameters/variables shown on host edit allows stored XSS in description to CVE-2015-7518 - Smart class parameters/variables shown on host edit allows stored XSS in description

- Description updated

#2 - 11/26/2015 06:58 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Assignee set to Tomer Brisker

- Pull request https://github.com/theforeman/foreman/pull/2936 added

#3 - 12/09/2015 09:01 AM - Anonymous

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 32468bce938067b1bbde1c2025771b5b83ce88ec.

#4 - 12/09/2015 10:21 AM - Dominic Cleal

- translation missing: en.field_release set to 63

#5 - 12/09/2015 11:04 AM - Dominic Cleal

The patch fixes a few distinct XSS paths in the same information popups:

1. Source name in global parameters, e.g. the name of a host group (since #7163 in 1.7.0)
2. Description field in smart variables/class parameters (since 1.2 or earlier)
3. Matcher in smart variables/class parameter overrides (since 1.2 or earlier)
4. Inherited value in smart variables/class parameter overrides (1.11/develop only, not released)

#6 - 12/09/2015 11:15 AM - Dominic Cleal

- Related to Feature #7163: In host's edit page, show the source for the value of puppet class parameters added

#7 - 01/21/2016 08:54 AM - Bryan Kearney

- Bugzilla link set to 1297040

#8 - 06/22/2016 09:09 AM - Dominic Cleal

- Related to Feature #15495: URL's in parameter description added