Foreman - Bug #2100

KS provisioning template regexp buffer overflow

01/03/2013 04:19 PM - Alejandro Falcon

Status:	Closed		
Priority:	Normal		
Assignee:	Dominic Cleal		
Category:	Templates		
Target version:	1.2.0		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

OS: Centos 6.3
Foreman version 1.1 RC3 from RPM

How to reproduce:
Create a new provisioning template with the content of the attached file.
Assign to a host and check it on templete review.
It ill show this message: "There was an error rendering the KS template: regexp buffer overflow"

Note: This was working ok on version 1.0.1.

Related issues:

Related to Foreman - Tracker #4656: Drop Ruby 1.8 support	**Closed**

Associated revisions

Revision d5226015 - 02/20/2013 06:00 AM - Dominic Cleal

fixes #2100 - fix regexp overflow on MRI 1.8 with older safemode/ruby_parser

History

#1 - 01/06/2013 01:53 PM - Alejandro Falcon

- File Gemfile.lock added

Attached Gemfile.lock

#2 - 01/08/2013 06:57 AM - Dominic Cleal

Confirmed on EL 6.4 with Foreman RC4, ruby_parser 3.0.1 (hm, should be 3.0.4) and safemode 1.1.0.

#3 - 01/08/2013 07:21 AM - Ohad Levy

does it work correctly on 3.0.4?

#4 - 01/08/2013 07:22 AM - Dominic Cleal

Ohad Levy wrote:

> does it work correctly on 3.0.4?

No, just tested ruby_parser 3.0.4 and it doesn't fix it, but it does work on a Fedora 17 system with Ruby 1.9.3 and either ruby_parser 3.0.1 or 3.0.4.

#5 - 01/17/2013 07:31 AM - Daniel Verniers

OS: Debian Squeeze 64bit
Foreman 1.1 RC4 from deb

I have the same problem with preseed provisioning templates.
finish and pxe templates are working fine, but provisioning is not working.

Are there any workarounds?

Thankx.

Daniel

#6 - 01/17/2013 07:32 AM - Daniel Verniers

There was an error rendering the TEMPLATE_NAME template: regexp buffer overflow

#7 - 01/17/2013 07:42 AM - Dominic Cleal

Daniel Verniers wrote:

> OS: Debian Squeeze 64bit
> Foreman 1.1 RC4 from deb
>
> I have the same problem with preseed provisioning templates.
> finish and pxe templates are working fine, but provisioning is not working.
>
> Are there any workarounds?

Disabling safemode_render under More->Settings->Provisioning is the only one I'm aware of. This means users with edit rights on provisioning templates can execute code in Foreman.

#8 - 01/17/2013 09:08 AM - Greg Sutcliffe

Daniel, do you have a sample preseed you can attach that shows the problem? be nice to cross-reference with the broken KS example.

#9 - 01/17/2013 09:46 AM - Daniel Verniers

@Dominic

This has solved the problem for the moment

@Greg Sutcliffe

I'll come back to your question later - i will create a minimal version of my preseed file as an example

#10 - 01/20/2013 01:17 PM - Ohad Levy

@Danial, please let us know, as I would consider this a blocker for 1.1 release

#11 - 01/30/2013 07:24 AM - Ohad Levy

- Target version deleted (1.1)

I don't consider this as a blocker for 1.1 release, since there is a workaround (which should be clearly documented in the release notes).

Since there is no trivial fix to resolved, I'm removing the 1.1 milestone from it.

#12 - 02/07/2013 06:56 AM - Anonymous

Dominic Cleal wrote:

> Ohad Levy wrote:
>
> > does it work correctly on 3.0.4?
>
> No, just tested ruby_parser 3.0.4 and it doesn't fix it, but it does work on a Fedora 17 system with Ruby 1.9.3 and either ruby_parser 3.0.1 or 3.0.4.

This is a stack overflow in 1.8.7 regex library. 1.9.3 is unaffected.

#13 - 02/12/2013 11:00 AM - Dominic Cleal

- Status changed from New to Assigned

- Assignee set to Dominic Cleal

I think to resolve this for MRI 1.8 we'll revert the versions of safemode and ruby_parser to their previous versions, but use the current version for MRI 1.9 where we need recent fixes to function.

#14 - 02/13/2013 05:22 AM - Dominic Cleal

- Status changed from Assigned to Ready For Testing

https://github.com/theforeman/foreman/pull/411

#15 - 02/18/2013 04:29 AM - Dominic Cleal

This is going to bring back #2217 (the warnings about redefined constants). Not sure if it's worth worrying about, or putting in our own code for defining the constants in Regexp so we don't hit the issue.

#16 - 02/20/2013 06:00 AM - Ohad Levy

- Target version set to 1.2.0

#17 - 02/20/2013 06:18 AM - Dominic Cleal

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset d52260159f1da0ea5341011c2c8705a7d75226ca.

#18 - 03/13/2014 05:39 PM - Dominic Cleal

- Related to Tracker #4656: Drop Ruby 1.8 support added

Files

ks-bug.txt	2.06 KB	01/03/2013	Alejandro Falcon
Gemfile.lock	3.52 KB	01/06/2013	Alejandro Falcon