Foreman - Bug #2109

session_token should not be static

01/05/2013 08:05 AM - Sandor Szücs

Status:	Closed		
Priority:	Immediate		
Assignee:	Dominic Cleal		
Category:	Users, Roles and Permissions		
Target version:	1.1		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

The session token of rails app should not be public available and static for all installations.

http://biggestfool.tumblr.com/post/24049554541/reminder-secret-token-rb-is-named-so-for-a-reason

Solution:
Generate the session token using SecureRandom, maybe as Rake Task, and add it to the installation and upgrade guides.
if RUBY_VERSION >= 1.9
require 'securerandom'
SecureRandom.urlsafe_base64(64)[0..63]
#=> "sZT3OdJVpHeIdbH5O8YLflOBXJbOv2ZY76GqsN1Clg1c1aiOzcMFZzKrRfUtJDTS"
else
...
end

Associated revisions

Revision adfcf8f0 - 01/08/2013 08:24 AM - Dominic Cleal

fixes #2109 - improve session token security

- adds security:generate token rake task to create static token
- generate and cache a token on startup if static token isn't present

Thanks to Sandor Szücs <sandor.szuecs@fu-berlin.de>

Revision 669affd3 - 01/25/2013 09:35 AM - Dominic Cleal

refs #2109 - generate secret token for cookies signing after install

Revision a0f490df - 02/04/2013 09:04 AM - Dominic Cleal

refs #2109 - generate secret token for cookies signing after install

Revision d775da09 - 02/04/2013 08:11 PM - Sam Kottler

Merge remote branch 'upstream/master' into rc_changes

- upstream/master:
  Further transition testing
  refs #2109 - generate secret token for cookies signing after install

Revision e2a34005 - 02/05/2013 08:33 AM - Dominic Cleal

refs #2109 - generate secret token for cookies signing after install

Revision a6dd55c2 - 02/05/2013 12:36 PM - Dominic Cleal

refs #2109 - restrict secret token to root:foreman

Revision a9f06590 - 02/06/2013 06:12 PM - Dominic Cleal

refs #2109 - restrict secret token to root:foreman, move before service start

History

#1 - 01/05/2013 04:50 PM - Ohad Levy

also, some more background http://blog.phusion.nl/2013/01/04/securing-the-rails-session-secret/

#2 - 01/06/2013 05:52 AM - Sandor Szücs

Ohad Levy wrote:

> also, some more background http://blog.phusion.nl/2013/01/04/securing-the-rails-session-secret/

I don't think that this: hash("#{machine_uuid}-#{hostname}-#{app_name}")
is good enough. If there are users with an operator role which have ssh access to look into logs or do some cleanup tasks that are not administrators in foreman webapp, then we have privilege escalation here. Hostname and app_name are known and uuid can be read with ssh access from a machine....
Anyway nice read, Ohad.

Greets Sandor

#3 - 01/06/2013 08:30 AM - Dominic Cleal

I like the rake task idea. To make it usable without running the task, we could comment out or delete secret_token.rb, then add an initializer after that generates + stores a key in tmp/ if the token's unset. People are then able to generate a static one with the rake task if they need it, which overrides the temporary secret.

#4 - 01/07/2013 09:32 AM - Dominic Cleal

- Status changed from New to Ready For Testing

Implemented the above, kept the rake task: https://github.com/theforeman/foreman/pull/353

Katello generates a secret during RPM installation too, we could do the same in our package post installs by running the rake task.

#5 - 01/07/2013 02:38 PM - Sandor Szücs

Dominic Cleal wrote:

> Implemented the above, kept the rake task: https://github.com/theforeman/foreman/pull/353
>
> Katello generates a secret during RPM installation too, we could do the same in our package post installs by running the rake task.

It's not a good idea to use activesupport's SecureRandom, because they removed it:
https://github.com/rails/rails/commit/1170cceaaec8c0c8aef173913405be1456e4b2be#activesupport/lib/active_support

#6 - 01/08/2013 09:52 AM - Dominic Cleal

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset adfcf8f0fa17dd352588fbd9eb24286502ccc90f.

#7 - 01/08/2013 10:12 AM - Ohad Levy

- Assignee set to Dominic Cleal

- Target version set to 1.1

Files

security.rake	1.22 KB	01/05/2013	Sandor Szücs