Foreman - Bug #6999

CVE-2014-3590 - User logout susceptible to CSRF attack

08/08/2014 03:25 AM - Dominic Cleal

Status:	Closed		
Priority:	Normal		
Assignee:	Daniel Lobato Garcia		
Category:	Security		
Target version:	1.6.1		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1110359	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/1738		

Description

I have created page on completely different machine with:

1. cat /var/www/html/pub/aaa.html
   <html>
   <body>
   <img src='https://foreman.example.com/users/logout&#039;/>
   </body>
   </html>

and once I have loaded it, I was logged-off from webUI.

Reported by Jan Hutař of Red Hat.

Related issues:

Related to Foreman - Bug #7736: Change to prevent unauthenticated requests fo...	**Rejected**	**09/29/2014**
Related to Foreman - Bug #7737: Change for issue 6999 broke logout for PAM-ba...	**Closed**	**09/29/2014**

Associated revisions

Revision 4e3a7e7a - 09/24/2014 05:42 AM - Daniel Lobato Garcia

Fixes #6999 - protect user logout against CSRF requests (CVE-2014-3590)

To avoid CSRF, logout is changed to be a POST request so
protect_from_forgery checks the CSRF token. However, in Rails 3 the only
strategy available is to nullify the session of the attacker.
We modify this behavior to raise a Foreman Exception.
This issue is probably worth revisiting on the update to Rails 4 as
throwing an exception is a valid strategy again.

Revision 4692b6bd - 10/07/2014 08:14 AM - Daniel Lobato Garcia

Fixes #6999 - protect user logout against CSRF requests (CVE-2014-3590)

To avoid CSRF, logout is changed to be a POST request so
protect_from_forgery checks the CSRF token. However, in Rails 3 the only
strategy available is to nullify the session of the attacker.
We modify this behavior to raise a Foreman Exception.
This issue is probably worth revisiting on the update to Rails 4 as
throwing an exception is a valid strategy again.

(cherry picked from commit 4e3a7e7a2a542435686a667773eafc73c92e557b)

History

#1 - 08/08/2014 06:45 AM - Dominic Cleal

- Subject changed from User logout susceptible to CSRF attack to CVE-2014-3590 - User logout susceptible to CSRF attack

CVE-2014-3590 has been assigned for this issue.

#2 - 08/21/2014 08:36 AM - Anonymous

- Target version changed from 1.7.5 to 1.7.4

#3 - 09/02/2014 12:05 PM - Shlomi Zadok

- Assignee set to Shlomi Zadok

#4 - 09/02/2014 12:08 PM - Shlomi Zadok

We should consider moving to devise (https://github.com/plataformatec/devise)

#5 - 09/03/2014 01:56 AM - Marek Hulán

+1 for devise, but since we have a lot of custom logic, it may be hard to rewrite it as warden strategies. Also devise does not seem to be packaged, it does not have many dependencies but still, another RPMs to maintain. IIRC correctly, katello used devise before enginification so maybe there are some older packages somewhere. Anyway implementing this fix probably shouldn't be a big rewrite.

#6 - 09/03/2014 06:15 AM - Dominic Cleal

- Status changed from New to Assigned

#7 - 09/03/2014 07:46 AM - Shlomi Zadok

- Status changed from Assigned to New

I have been looking into this issue.
This happens only on the browser that you are logged in your foreman webUI.
(e.g., if you are on Chrome and logged in a foreman webUI, you will be logged out if you clicked on a logout link on another tab).
The logout link can be on another server (as Dominic described).

This will not happen on another browser (you won't be able to logout a Chrome foreman webUI from FireFox).

Yet, this seems to me as a normal behavior of the browsers, If I am logged out from Facebook on one tab, it will log me out from Facebook on other tabs as well.

As for devise, clearly an issue we should consider in the future.

#8 - 09/03/2014 07:51 AM - Dominic Cleal

It's a CSRF attack though, that's a preventable behaviour with CSRF tokens etc, in the same way that forms are protected.

#9 - 09/04/2014 12:48 PM - Dominic Cleal

- translation missing: en.field_release changed from 20 to 22

#10 - 09/05/2014 05:08 AM - Daniel Lobato Garcia

- Assignee changed from Shlomi Zadok to Daniel Lobato Garcia

#11 - 09/05/2014 06:32 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Pull request https://github.com/theforeman/foreman/pull/1738 added

- Pull request deleted ()

#12 - 09/10/2014 07:22 AM - Anonymous

- Target version changed from 1.7.4 to 1.7.3

#13 - 09/24/2014 06:01 AM - Daniel Lobato Garcia

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 4e3a7e7a2a542435686a667773eafc73c92e557b.

#14 - 09/29/2014 10:15 AM - Dominic Cleal

- Related to Bug #7736: Change to prevent unauthenticated requests for CSRF modified login behaviour as well added

#15 - 09/29/2014 10:23 AM - Marek Hulán

- Related to Bug #7737: Change for issue 6999 broke logout for PAM-based (intercept) authentication added