Redmine - Patch #17717
Password/Email address change should invalidate security tokens

2014-08-20 16:21 - Jan from Planio www.plan.io

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Baptiste Barth	**% Done:**	90%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	2.6.0		

Description

To improve user account security, we believe it is a good practice to:

1. **invalidate the password reset token** (sent via email) once an account's **email address is changed**.
   (This prevents hackers who may be able to change a user's address (or trick him into doing it) to use an "old" password reset link previously sent via email once the email address has been changed back by the user.)
2. **invalidate the password reset token** and **autologin token** once an account's **password is changed**.
   (This prevents hackers from being still able to login after a user has potentially discovered a breach into his/her account and changed their password.)

The attached patch against current Redmine trunk implements this; tests included.

Associated revisions

Revision 13396 - 2014-09-14 10:22 - Jean-Baptiste Barth

Invalidate security tokens on password or email changes (#17717).

Contributed by Jan Schulz-Hofen.

Revision 13403 - 2014-09-14 13:38 - Jean-Philippe Lang

Code cleanup (#17717).

History

#1 - 2014-09-04 19:03 - Jan from Planio www.plan.io

- % Done changed from 0 to 90

#2 - 2014-09-08 22:12 - Jean-Baptiste Barth

- Assignee set to Jean-Baptiste Barth

Looks good, and I confirm tests pass! There's just a little typo in the comment but nothing serious.

I'd like to have details by Jean-Philippe about how we deal with that kind of security improvements: I was about to commit it but it may not be a good idea weeks or months before a new major version is released. Jean-Philippe ?

#3 - 2014-09-09 15:00 - Jan from Planio www.plan.io

Jean-Baptiste Barth wrote:

> *Looks good, and I confirm tests pass! There's just a little typo in the comment but nothing serious.*

Thanks.

> *I'd like to have details by Jean-Philippe about how we deal with that kind of security improvements: I was about to commit it but it may not be a good idea weeks or months before a new major version is released. Jean-Philippe ?*

Personally, I don't think it would be a problem since it's not a fix for a security issue per se. Both this and #17796 can only be exploited in conjunction with social engineering or other security problems and not by itself. But I agree, let's wait for Jean-Philippe's opinion on this!

#4 - 2014-09-13 11:54 - Jean-Philippe Lang

Jan from Planio www.plan.io wrote:

> *Personally, I don't think it would be a problem since it's not a fix for a security issue per se. Both this and #17796 can only be exploited in conjunction with social engineering or other security problems and not by itself. But I agree, let's wait for Jean-Philippe's opinion on this!*

Agreed, this change and #17796 can be committed now for 2.6. Thanks.

#5 - 2014-09-13 14:28 - Etienne Massip

Why are both issues in Security? Do you have any objection if we move them to public?

More generally, now that issues can be set as private, do we still need Security project?

#6 - 2014-09-13 14:43 - Jan from Planio www.plan.io

Etienne Massip wrote:

> *Why are both issues in Security? Do you have any objection if we move them to public?*

It was just a precautionary measure. In theory, the issues can be exploited (together with some other vector such as social engineering), so I wanted to be sure to not tell more people about this as necessary before a fix is available for Redmine admins.

It may make sense to mov security issues to the public Redmine project, once they're fixed and released, to increase transparency. (Or we use the private flag as you suggest and remove it once released.)

#7 - 2014-09-13 22:23 - Etienne Massip

- Project changed from Security to Redmine
- Category set to Security
- Target version set to 2.6.0

#8 - 2014-09-14 10:24 - Jean-Baptiste Barth

- Status changed from Needs feedback to Closed

Committed it in r13396.

#9 - 2014-09-14 10:36 - Jan from Planio www.plan.io

Thanks!

Files

0001-Delete-tokens-on-mail-or-password-change.patch	3.18 KB	2014-08-20	Jan from Planio www.plan.io