Redmine - Defect #13197
Don't send password in plain text via email after registration

2013-02-17 20:10 - Martin Eberle

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Cant reproduce	**Affected version:**	

Description

When the registration process is set to manual account activation, the new user gets automatically an email with his (self set) username and password in plain text.

This is a dangerous security risk!

And it is not necessary. The user knows the password anyway, because it was set by himself.

Related issues:

Related to Redmine - Patch # 21436: Prevent admins from sending themselves th...	**Closed**

History

#1 - 2013-02-17 22:27 - Jean-Philippe Lang

- Priority changed from High to Normal

AFAIK, it's only when an admin changes a user's password that it can be sent by email. Could you give the steps to reproduce your issue?

#2 - 2013-02-19 02:48 - Toshi MARUYAMA

- Tracker changed from Patch to Defect

#3 - 2013-02-20 22:11 - Jean-Philippe Lang

- Resolution set to Cant reproduce

#4 - 2013-02-27 15:47 - Martin Eberle

Jean-Philippe Lang wrote:

> *AFAIK, it's only when an admin changes a user's password that it can be sent by email. Could you give the steps to reproduce your issue?*

I just tried to reproduce it but i wasn't successful. I think it happens during the installation of Redmine when the admin sets up his account. In this case the self set password is sent via email.

#5 - 2015-04-12 03:00 - Go MAEDA

- Status changed from New to Closed

Since nobody can reproduce it, I am closing this issue.

#6 - 2015-12-06 12:11 - int redmine

I can reproduce this on redmine 3.1.3.
It is as the original issue opener said:
When the registration process is set to manual account activation, the new user gets automatically an email with his (self set) username and password in plain text.

This happens when the admin activates the account. In this case it is not necessary since the user knows the password anyway, because it was set by himself.
It also happens when a users password is overwritten by admin with a new password.
In this case it would be good to have a option change that behaviour. Sending of plain text password should be disabled by default and only be done if admin enables this feature.

Please reopen this issue.

#7 - 2015-12-06 16:57 - Jan from Planio www.plan.io

- File send_account_info.png added

I have just revisited this issue due to a tweet. I am not able to reproduce it either.

Martin Eberle wrote:

> *When the registration process is set to manual account activation, the new user gets automatically an email with his (self set) username and password in plain text.*

This does not seem to be the case. I've now tested this and revisited the code again. The password entered during manual registration is **not** sent when a users registers for a new account.

int redmine wrote:

> *This happens when the admin activates the account. In this case it is not necessary since the user knows the password anyway, because it was set by himself.*

This is technically not possible. The plain text password is only kept in memory during the Account#register request and never gets stored in the database. Since passwords are hashed, there is no way to compute a plain text password from its stored hash. Therefore, during activation by an admin, the plain text is not available anymore and cannot possibly be sent via email.

int redmine wrote:

> *It also happens when a users password is overwritten by admin with a new password.*

This particular aspect is correct and intended behavior. If the admin sets a new password, there should be a way to tell that new password to the user.

int redmine wrote:

> *In this case it would be good to have a option change that behaviour. Sending of plain text password should be disabled by default and only be done if admin enables this feature.*

There is an option for the admin already to select whether or not the account information (including password) should be sent or not. There is also an option to require the user to change the (insecurely transmitted) password at her first login – see screenshot.

{{thumbnail(send_account_info.png, size=419)}}

Please clarify how you were able to reproduce this. Otherwise, I don't think we should reopen this issue.

#8 - 2015-12-06 17:28 - Jan from Planio www.plan.io

Martin Eberle wrote:

> *Jean-Philippe Lang wrote:*
>
> > *AFAIK, it's only when an admin changes a user's password that it can be sent by email. Could you give the steps to reproduce your issue?*
>
> *I just tried to reproduce it but i wasn't successful. I think it happens during the installation of Redmine when the admin sets up his account. In this case the self set password is sent via email.*

Aha! The problem you describe here is actually quite different from your initial description in this issue, but it's still a valid (albeit much less severe) concern. I've opened #21436 for it and proposed a patch. Thanks!

#9 - 2015-12-06 17:34 - Jan from Planio www.plan.io

- Related to Patch #21436: Prevent admins from sending themselves their own password added

Files

send_account_info.png	48.3 KB	2015-12-06	Jan from Planio www.plan.io