Redmine - Defect #17830

User creation: clear/plaintext password sent via unencrypted email

2014-09-10 13:44 - Hendrik Jaeger

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Baptiste Barth	**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	Candidate for next major release		
Resolution:		**Affected version:**	1.4.4

Description

```
  henk | I just received an unencrypted mail from redmine containing my password in plaintext. Is
that fixed in more recent versions? Is there a way to fix it in 1.4.4?
  henk | https://twitter.com/RamsayDev/status/460048737994551296 hehe, yeah, kinda my thoughts …
salvor | henk: no.
salvor | henk: that's only on user creation, and it's up to the administrator to send this passwor
d or not
salvor | after that everything happen through tokens
  henk | salvor: hm, ok, that’s not too bad then, but I still wonder why that’s not done through t
okens as well?!
salvor | I guess we could do that even on user creation (= send a unique link to reset the passwor
d) ; or force password change on first connection (which is the same security wise I think)
salvor | do you see a legitimate case where an administrator would want to set a password manually
 for a user ?
  henk | salvor: No, not really. IMHO it’s nice to have that feature and I wouldn’t want it to go
away, but it’s not a good default way to handle things.
salvor | I totally agree
```

Another idea:
allow specifying a pgp-key and send the mail encrypted

History

#1 - 2014-09-10 13:50 - Jean-Baptiste Barth

- Assignee set to Jean-Baptiste Barth

- Target version set to Candidate for next major release

Taking it as salvor == me :) Any comment welcome.

#2 - 2014-09-20 00:06 - Michael Weinberg

More problems- I'm running v 2.5.2:
1. There is a checkbox ("Send account information to the user") that is checked by default and unchecking it doesn't stick.

2. I changed my password for an existing account and it send it plain text.

3. There is no indication that "account information" contains the plain text password. At the very minimum, any password sent via plain text should be assumed compromised- The user should be required to change the password if they ever get a password in plain text.

#3 - 2020-11-01 14:51 - Michael Gerz

Does this security issue still exist after so many years?

#4 - 2023-05-03 11:41 - Hendrik Jaeger

I just registered a new account here on redmine.org and only received the registration link.
When I reported this, it was version 1.4.4, it seems, now we are at major version 4/5.

It seems like at least part of this issue is fixed.
Jean-Baptiste Barth can you provide a more complete and/or accurate update?

#5 - 2023-05-04 02:39 - Go MAEDA

Hendrik Jaeger wrote in #note-4:

> I just registered a new account here on redmine.org and only received the registration link.
> When I reported this, it was version 1.4.4, it seems, now we are at major version 4/5.
>
> It seems like at least part of this issue is fixed.

No, it is not yet fixed. Even in Redmine 5.0, a password will be sent in plain text if an administrator checks the checkbox named "Send account information to the user" when creating a user.

#6 - 2023-05-04 16:43 - Holger Just

It may be a good idea to force users to change the password on first login if the password was sent to the user. Then, the initial password is effectively a token which allows the user to login once.

This could be enforced by setting the must_change_password flag on the user (and thus implicitly enable the respective checkbox on the users/new.html.erb form) if account details are sent to the user. This could be added in the UsersController. We also might add some documentation to explain what this does and note that the email will include the generated or set password.

Hendrik Jaeger wrote in #note-4:

> I just registered a new account here on redmine.org and only received the registration link.
> When I reported this, it was version 1.4.4, it seems, now we are at major version 4/5.
>
> It seems like at least part of this issue is fixed.

As far as I understand the old code, in Redmine < 3.4 we have indeed checked the "Send account information to the user" checkbox by default. Unless the administrator has actively unchecked the checkbox each time, the password of the new user would indeed be sent via plaintext mail by default. I believe this was incidentally changed in r16453 so that this checkbox is not checked by default.

In any case, as far as I'm aware, when self-registering, we have never sent the self-selected password via mail. This was (and still is) only used as a way to sent the newly created user a means to login if this new user was created by an admin.