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 password 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 tokens as well?!
salvor | I guess we could do that even on user creation (= send a unique link to reset the password) ; 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.