Redmine - Feature #28724

Reset the API key when changing/resetting user passwords?

2018-05-09 16:38 - Martin von Wittich

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:			
Resolution:			

Description

At the moment, Redmine won't reset the API key when a user changes his own password, or when an administrator resets the user's password. As far as I can tell, administrators don't even have the ability to reset API keys of users; only the users themselves can reset their API keys.

Doesn't this pose a security problem for sites where API access has been enabled? Assume for example that a user account has been hacked, and either the user or the administrator changes the user's password. Now the user/administrator might assume that the situation has been resolved, but in fact the user still has to manually reset his API key, because the attacker might have saved it. If the user doesn't do this (for example because he doesn't know about the API key at all), he now left his account open to API abuse by the attacker.

Maybe the password dialog should display a note about this, or offer a check box that resets the API key?

History

#1 - 2024-08-17 08:22 - Marco Descher

This is a security problem, I wonder that this was never considered!