

redmineorg-copy202205 - Vote #79304

Reset the API key when changing/resetting user passwords?

2022/05/09 18:32 - Admin Redmine

ステータス:	New	開始日:	2022/05/09
優先度:	通常	期日:	
担当者:		進捗率:	0%
カテゴリ:	Accounts / authentication_7	予定工数:	0.00時間
対象バージョン:		作業時間:	0.00時間
Redmineorg_URL:	https://www.redmine.org/issues/28724	status_id:	1
category_id:	7	tracker_id:	2
version_id:	0	plus1:	0
issue_org_id:	28724	affected_version:	
author_id:	153583	closed_on:	
assigned_to_id:	0	affected_version_id:	
comments:	0		

説明

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?

履歴

#1 - 2022/05/10 17:04 - Admin Redmine

- カテゴリ を Accounts / authentication_7 にセット