redmineorg-copy202205 - Vote #72655

Users can easily use any (not yet used) email address for their account (potential security issue)

2022/05/09 16:25 - 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/12106	**status_id:**	1
category_id:	7	**tracker_id:**	1
version_id:	0	**plus1:**	2
issue_org_id:	12106	**affected_version:**	
author_id:	4	**closed_on:**	
assigned_to_id:	0	**affected_version_id:**	
comments:	7		

説明

When a user registers a new account, Redmine verifies the user's email address via the standard authentication email scheme: User gets an email to the claimed email address with a authentication code resp. a URL containing this authentication code; the user can only proceed with registration using that email address when he can actually read emails sent to this email address.

This serves two purposes:

Users are prevented from accidentally mistyping the email address.

Users are prevented from maliciously associating somebody else's email address with an account they control.

The problem: Redmine currently only performs this check when registering an account. Once one has registered an account (e.g. by using a temporary email address such as "10 Minute Mail"), one can freely change the email address associated to the account without any further checks; the only exception is that email address which are already in use cannot be used.

This allows for abuse and mistakes in multiple ways:

- Users may want to change their email address, and accidentally introduce a typo without noticing.
- Attackers could use this to claim the identity of a victim, as described above.
- Attackers could use this to prevent a victim from signing up with their email address if they are quicker in registering an account. This could be used to prevent the actual owner of that email address to register an account; or to post fake comments in the name of actual owner (the "victim") of the email address. The latter could be done in an attempt to abuse the good reputation of the victim (e.g. the attacked could pretend to be Linus Torvalds...) or to worsen the reputation of the victim by, say, by posting inflamatory messages in victim's name.

To solve this, the validity of the email address should be verified upon any change (perhaps optional based upon a site wide setting, but I think this should be on by default).

Of course this creates some potential UI difficulties. For example, which email address should Redmine use in the time between the request to change the address, until the verification happens -- and what if the verification never happens? Perhaps there should be a "timeout" then on each change request? What if there is another change request while the first one is still pending?

A more natural way might to overcome this might be to allow for multiple emails per user (something that has been requested before (see issue #4244). In this model, one cannot "change" the email address, merely add email addresses (each time using proper verification; and using the same code as during registration), select one of the verified email addresses as "default" (notifications go to this address), and remove any address (except for the default address). Each of these individual operations is quite basic and easy to implement right, and avoids all the headaches of a safe system for changing a single email address.

This is also the model employed by GitHub, see https://github.com/settings/emails (you have to be logged on there to see the UI).

journals

And just to demo the problem... Hi, I am of course not Bill Gates... Feel free to delete this account.

+1

Bill Gates wrote:

> And just to demo the problem... Hi, I am of course not Bill Gates... Feel free to delete this account.

Nice try, but we're still not buying Team Foundation Server

+1

Just to clarify, when I wrote "and using the same code as during registration" what I meant was "and using the same authentication code scheme as during registration" -- of course the actual code / hash key being used should not be the same!

Ah, and also sorry for all those embarrassing typos and cut&paste artifacts, but I hope that the overall idea is understandable.

+1

Note: my "fake Bill Gates" has been deleted, but before that, the first comment was looking as if it was by a user named "Bill Gates" with email address "bill@microsoft.com".

---

related_issues

relates,Closed,12855,Sometime,we need limit register email address

履歴

#1 - 2022/05/10 17:15 - Admin Redmine

- カテゴリ を Accounts / authentication_7 にセット