

privacy problem on users info

2022/05/09 19:10 - Admin Redmine

ステータス:	Needs feedback	開始日:	2022/05/09
優先度:	通常	期日:	
担当者:		進捗率:	0%
カテゴリ:		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/34593	status_id:	10
category_id:	0	tracker_id:	1
version_id:	0	plus1:	0
issue_org_id:	34593	affected_version:	
author_id:	141725	closed_on:	
assigned_to_id:	0	affected_version_id:	160
comments:	3		

説明

If a logged-in user starts to access cyclically to URLs like this:

```
https://example.com/redmine/users/5
https://example.com/redmine/users/6
https://example.com/redmine/users/7
...
```

he/she will see and get the full organization's users, members, informations, accounts, email etc... This is a particular sensible information if the organization needs to hide and protect membership information from all users.

This looks like a violation of privacy information. Also the organization cannot hide to any member this wide information. Looks like a design lack.

journals

Can you access all those information using an user without permissions?

Marius BALTEANU wrote:

Can you access all those information using an user without permissions?

I can, from my (presumably) unprivileged acct. The 'hide email address' feature seems to work though. Maybe need to add more 'hide [data]' options for other sensitive data fields?

Michael Troester wrote:

Marius BALTEANU wrote:

Can you access all those information using an user without permissions?

I can, from my (presumably) unprivileged acct. The 'hide email address' feature seems to work though. Maybe need to add more 'hide [data]' options for other sensitive data fields?

You already have the following settings:

1. Users visibility (All active users / Members of visible projects) at role level.
2. The "hide email address" already mentioned by you.
3. "Users display format" global setting to control how to show the user based on First name and Last name.

which covers all the users standard fields. If you want to be very strict about who have access to user's info, maybe you should review the setting from 1 for all roles.

Regarding more 'hide [data]', do you have custom fields for users? If yes, that make sense to have the same options to configure the custom field visibility as already exists for issues, spent time, versions or projects.