Redmine - Defect #14650

Security vulnerability in Redmine REST API

2013-08-08 22:33 - Wesley Falcao

Status:	Closed	**Start date:**	
Priority:	Urgent	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Invalid	**Affected version:**	2.3.2

Description

If I login as a non-administrator and try -

http://localhost:3000/users/

I get a 403 error saying "You are not authorized to access this page".

However, logged in as the same user, I can do

http://localhost:3000/users/1.xml
http://localhost:3000/users/2.xml
...
...
...
http://localhost:3000/users/n.xml

And I can access all the users, including their api keys.

History

#1 - 2013-08-09 12:24 - Jean-Philippe Lang

- Private changed from No to Yes

#2 - 2015-11-27 09:31 - Jan from Planio www.plan.io

- Status changed from New to Closed

- Private changed from Yes to No

- Resolution set to Invalid

Wesley Falcao wrote:

> If I login as a non-administrator and try -
>
> http://localhost:3000/users/
>
> I get a 403 error saying "You are not authorized to access this page".

That is intended. There is no public user list for non-admins. /users is the regular admin's user view. This might be seen as a missing feature but not a security problem.

> However, logged in as the same user, I can do
>
> http://localhost:3000/users/1.xml
> http://localhost:3000/users/2.xml
> ...
> ...
> ...
> http://localhost:3000/users/n.xml

This also works "as intended". Users are also able to use the non-API version of these links to see the same details:

- http://localhost:3000/users/1
- http://localhost:3000/users/2, etc.

Users can define however in their *My Account* page if their email address may be shown on these pages or not.

> And I can access all the users, including their api keys.

Nobody here was able to reproduce this particular claim. API keys are only shown if you are in fact admin or if you are looking at your own user.