Redmine - Defect #18842

Updating issue possible for a user without that permission

2015-01-15 01:33 - djiby thiaw

Status:	Closed		**Start date:**	
Priority:	Normal		**Due date:**	2015-09-05
Assignee:			**% Done:**	0%
Category:	Issues permissions		**Estimated time:**	0.00 hour
Target version:				
Resolution:			**Affected version:**	2.6.1

Description

Hi,
For a specific user, I don't give to him the permission to edit an issue. Now in the tasks page, when he rigth clicks on an issue, the button edit is disable. The problem is that when he clicks on the issue (show issue), The button edit on top right is now enabled and he can edit the issue and save changes.

History

#1 - 2015-01-15 03:57 - Toshi MARUYAMA

- Status changed from New to Needs feedback

See Submissions.

Check what his role is.
And check his and non members' and anonymous' permissions.

#2 - 2015-01-15 22:36 - djiby thiaw

- File permissions_on_issue.png added

- File edit_in_task_show.png added

- File edit_with_right_click.png added

Hi
With these linked screen shots you can clearly see what is the problem
I'm using ruby 1.9.3, and rails 3.2.19. For the DB it is 5.5.40-MariaDB

#3 - 2015-01-18 07:46 - Mischa The Evil

This is in fact the 'expected' behavior whenever the role has been given the "Add notes" permission (which corresponds with@:add_issue_notes@ [source:/trunk/lib/redmine.rb@13892#L107]) as your screenshots show. I'll elaborate.

When the issues context menu is being rendered, the (bulk-)edit elements are marked *disabled* based on the condition !@can[:edit] (source:/trunk/app/views/context_menus/issues.html.erb@13892#L4). This condition is met if the user misses the :edit_issues permission for *any* project inside the @projects array (source:/trunk/app/controllers/context_menus_controller.rb@13892#L32, where @projects is defined in the #find_issues before filter).

Whenever we talk about the "Edit" button on the single issue view (source:/trunk/app/views/issues/show.html.erb@13892) the situation is different. This specific button is rendered as part of a separate partial, only whenever @issue.editable? returns true (source:/trunk/app/views/issues/_action_menu.html.erb@13892#L2), which is the case when the user either has the :edit_issues or the :add_issue_notes permission for the current issue's project (source:/trunk/app/models/issue.rb@13892#L154).

Now, to come back to your scenario, you have a user who is granted the :add_issue_notes permission, but not the :edit_issues permission. As outlined above the user sees the regular "Edit" button on the single issue view. Clicking this button will lead them to a form where only the "Notes" fieldset is available (because they need to be able to add notes to issues) and where rendering of the "Change properties" fieldset is omitted, as such *preventing them from editing issue properties*. This "Change properties" fieldset is rendered only if the user has the :edit_issues permission.

So, in the end this seems to be just an UI issue regarding the "Edit" element of the issues context menu which does not consider the same permission set as the "Edit" button on the issues show view does.

#4 - 2015-01-20 00:17 - djiby thiaw

Hi,
I've a little bit understand what you explain. And also an other think is that for a role i give hime the permission to just view the issues created by him or assigned to him. But in the issues list, all the issues created appear and the user will have a 403 -No authorized just when he clicks on the issue for

details. Is it possible to don't show in the list the issues that he didn't create or not assigned to him.
Thanks

#5 - 2015-08-23 16:56 - Jan Niggemann (redmine.org team member)

- Due date set to 2015-09-05

Is this issue resolved?

#6 - 2015-09-11 07:53 - Toshi MARUYAMA

- Status changed from Needs feedback to Closed

djiby thiaw wrote:

> Hi,
> I've a little bit understand what you explain. And also an other think is that for a role i give hime the permission to just view the issues created by
> him or assigned to him. But in the issues list, all the issues created appear and the user will have a 403 -No authorized just when he clicks on the
> issue for details. Is it possible to don't show in the list the issues that he didn't create or not assigned to him.

This is not related with description.
Please create new issue if you still have problem.

Files

permissions_on_issue.png	17.9 KB	2015-01-15	djiby thiaw
edit_in_task_show.png	3.77 KB	2015-01-15	djiby thiaw
edit_with_right_click.png	14 KB	2015-01-15	djiby thiaw