Redmine - Defect #15789

Users can see all groups when adding a filter "Assignee's Group"

2013-12-31 14:42 - Pierre Maigne

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	Permissions and roles	**Estimated time:**	0.00 hour
Target version:	3.0.0		
Resolution:	Fixed	**Affected version:**	2.4.2

Description

Hello,

I'm going to quote Djordjije who perfectly explained the problem in issue #11724, note 13 (even if issue #11724 has nothing to do with this current issue).

Djordjije Crni wrote:

> User can see the names of all groups on Redmine, by selecting issue filter by "Assignee's group"!
> This happens even if issue assignment to groups isn't allowed.
> I've expected to see only the names of those groups which are assigned to that project in the filter list.
> And guess what, almost all group names (in my case) are constructed from two parts: project role and project name. Very original idea, isn't it?
> In this case, customer can easily guess names of all projects, which is not acceptible at all.
> It seems that current Redmine user/group permission model can't provide reliable customer/project isolation.
> "Workaround" could be to give meaningless names to groups, and even better, give meaningless names to projects also?

We have the same issue. We create a group for each customer who is accessing Redmine, and the group name is the customer name. This way, any customer can access our whole customer list.

Thanks in advance for your feedback.

Related issues:

Related to Redmine - Feature #11724: Prevent users from seeing other users ba...	**Closed**

History

#1 - 2013-12-31 21:12 - Mischa The Evil

- Related to Feature #11724: Prevent users from seeing other users based on their project membership added

#2 - 2014-01-21 14:32 - Markus Peter

A solution would be to *only list groups which are linked to a role in the current project*.

In our case (a group for each client), this would effectively prevent our clients from seeing each other.
We now have to link all client users directly to their projects in order to bypass the creation of a group.

#3 - 2014-05-19 11:10 - Rafał Lisowski

- File 0001-redmine-issue-15789.patch added

I just disabled filter by group. No one use it at my company so it was the easiest way to prevent data leakage.
I don't have time now to impelement Marcus Peter solution: "only list groups which are linked to a role in the current project".

#4 - 2014-11-11 14:22 - Jean-Philippe Lang

- Status changed from New to Closed

- Assignee set to Jean-Philippe Lang

- Target version set to 3.0.0

- Resolution set to Fixed

Fixed by r13584. Depending on Users visibility setting on roles, the group filter will list groups linked to visible projects only.

Files

0001-redmine-issue-15789.patch	1.14 KB	2014-05-19	Rafał Lisowski