Redmine - Feature #11724
Prevent users from seeing other users based on their project membership

2012-08-28 10:11 - Maxim Kim

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		

Description

This feature #5159 caused a major problems at least for us.
We let our customers to add new issues and watchers. And now our customers can see other customer names, which is inacceptable!
Could you please add asap setting to switch off this feature.

My personal opinion is that right solution was to add permission "can be non-member watcher" as someone suggested earlier.

Related issues:

Related to Redmine - Feature # 5159: Ability to add Non-Member watchers to th...	**Closed**	**2010-03-23**
Related to Redmine - Feature # 13527: 'Display name' for users	**New**	
Related to Redmine - Feature # 13533: Concept for controlling visibility of u...	**New**	
Related to Redmine - Defect # 9500: Watchers list before and after creation i...	**New**	**2011-10-31**
Related to Redmine - Defect # 15789: Users can see all groups when adding a f...	**Closed**	
Related to Redmine - Feature # 17747: Private roles	**New**	
Related to Redmine - Patch # 18128: Make User profile 404 rendering more cons...	**Closed**	
Related to Redmine - Feature # 6015: Private Users	**New**	**2010-08-02**
Related to Redmine - Feature # 26555: Hide user information from other users ...	**New**	
Duplicated by Redmine - Defect # 15123: "Add watcher" leaks all active users	**Closed**	

Associated revisions

Revision 13584 - 2014-11-11 14:08 - Jean-Philippe Lang

Adds a role setting for controlling visibility of users: all or members of visible projects (#11724).

Revision 13585 - 2014-11-11 14:10 - Jean-Philippe Lang

Adds strings to locales (#11724).

Revision 13586 - 2014-11-11 14:18 - Jean-Philippe Lang

Display visible users only for when adding project members (#11724).

History

#1 - 2012-08-28 15:58 - William Roush

This almost sounds like it should be the other way around:

The permission should probably be on the user to add non-member watchers. If I'm a project manager I can't be limited for something that in essence

is to keep non-members from adding each other.

Of course does this mean that non-members can view profiles of other non-members? If so this permission would be pretty useless, I can just cruise the member list if this barrier is put in place (which means this issue has really existed for a *long* time).

I'd almost suggest the ability to limit users from seeing non-members in general, and let that permission cascade to this search box.

#2 - 2012-08-28 16:49 - Etienne Massip

- Tracker changed from Defect to Feature
- Subject changed from Re: Ability to add Non-Member watchers to the watch list to Prevent users from seeing other users based on their project membership
- Category changed from Administration to Permissions and roles
- Assignee deleted (Jean-Philippe Lang)
- Priority changed from High to Normal
- Target version set to Candidate for next major release

#3 - 2012-09-08 12:41 - Hannes Meier

whaaaaaaaaat????

that s really not good. i just set up a redmine for 2 customers and you are absolutely right, they can see each other if they add watchers.

Same for the redmine/users/XX links.
Everyone can scan all users at any time. A role/permission to change that would be very important.

#4 - 2012-11-20 11:44 - Dries Maertens

You should check out http://www.redmine.org/boards/1/topics/4143
They post a solution to manually change some files to change what certain members can see.

I still think this should remain a feature for a future version so we don't have to do this in the code directly.

#5 - 2013-03-19 16:47 - Tobias Fischer

+1 on this feature-request!

We're having the same problem as Maxim.
But I think that a role-permission is the wrong way to do this!

This should be a **project specific option!**

#6 - 2013-08-14 04:39 - Mischa The Evil

Maxim Kim wrote:

> *This feature #5159 caused a major problems at least for us.*
> *We let our customers to add new issues and watchers. And now our customers can see other customer names, which is inacceptable!*
> *[...]*

This is true defect IMO. As a workaround you can revoke the "Add watchers" permission from your customer roles.

William Roush wrote:

> *Of course does this mean that non-members can view profiles of other non-members? If so this permission would be pretty useless, I can just cruise the member list if this barrier is put in place (which means this issue has really existed for a long* time).
>
> I'd almost suggest the ability to limit users from seeing non-members in general, and let that permission cascade to this search box.

Hannes Meier wrote:

> *[...]*
>
> *Same for the redmine/users/XX links.*
> *Everyone can scan all users at any time. [...]*

It is simply *not true* that all users can browse account/user pages unlimited. This is reserved to administrators only. Non-admin users can't browse user pages of users who are not active ánd who have no visible project or activity. See #14601#note-1 (note-1) and more historically r2986 (for #4129 & #3720).

#7 - 2013-10-14 10:33 - Mischa The Evil

- Related to Defect #15123: "Add watcher" leaks all active users added

#8 - 2013-10-20 17:49 - Jean-Philippe Lang

- Assignee set to Jean-Philippe Lang

Rather than adding a specific permission for adding non members as watchers, I'd like to add a setting on each role that defines which users the role is allowed to see: all users or members of visible projects. That would apply to adding watchers and viewing users as well (/users/:id). And I think it would be easier for those who want to control user visibility (rather than reviewing all permissions to know which users the role can see).

#9 - 2013-10-21 05:34 - Mischa The Evil

Jean-Philippe Lang wrote:

> *[...] I'd like to add a setting on each role that defines which users the role is allowed to see: all users or members of visible projects [...]*

I think that would be a good solution for this issue.

#10 - 2013-10-21 09:09 - Maxim Kim

That is great news but we had to go with different software already because of that.
But good to know, if this is fixed in future we may consider a comeback.

Maxim Kim wrote:

> *Added by Maxim Kim about 1 year ago.*

#11 - 2013-10-21 13:14 - Etienne Massip

Jean-Philippe Lang wrote:

> *Rather than adding a specific permission for adding non members as watchers, I'd like to add a setting on each role that defines which users the role is allowed to see: all users or members of visible projects. That would apply to adding watchers and viewing users as well (/users/:id). And I think it would be easier for those who want to control user visibility (rather than reviewing all permissions to know which users the role can see).*

I think this should not solve the critical case where reporters of a private project are external customers that should not know who are the other customers, would it?

And when an user is not tied to a project anymore, you can't have any visibility policy applicable, right ?

Why not simply have a "public"/"private" user setting(which could be extended to group) and have a "See private users" setting at role level?

Edit: actually, it was described by Joshua in #13533.

#12 - 2013-10-30 11:01 - Toshi MARUYAMA

- Related to Defect #9500: Watchers list before and after creation issue added

#13 - 2013-11-07 00:36 - Djordjije Crni

First of all, I would like to thank to Felix Schäfer, who provided a patch for Defect #15123 *"Add watcher" leaks all active users* issue.
Today we've found one more serious problem with user & groups visibility. (We are using Redmine v2.3.3 at the moment.)
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?

Debug log shows following SQL query for groups:

```
SELECT "users".* FROM "users" INNER JOIN "groups_users" ON "users"."id" = "groups_users"."group_id" WHERE "users"."type" IN ('Group') AND "groups_users"."user_id" = 1
```

The code is somewhere in app/models/issue_query.rb, as far as I can see.
The query should show only groups which are members of project, not all groups, something like:

```
SELECT "members"."id" AS t0_r0, "members"."user_id" AS t0_r1, "members"."project_id" AS t0_r2 ... FROM "members" LEFT OUTER JOIN "users" ON "users"."id" = "members"."user_id" WHERE "members"."project_id" = 1 AND (users.type='Group')
```

#14 - 2013-12-06 14:50 - Toshi MARUYAMA

- Related to deleted (Defect #15123: "Add watcher" leaks all active users)

#15 - 2013-12-06 14:50 - Toshi MARUYAMA

- Duplicated by Defect #15123: "Add watcher" leaks all active users added

#16 - 2013-12-31 14:21 - Pierre Maigne

This issue is also affecting us. Our customers have access to Redmine for their respective projects, but we don't really want them to access the global user list.
Until we have a solution, we removed the "Add Watchers" role, but it would better if that role was open to our customers.

I'm also going to open a separate ticket for the issue described by Djordjije 3 comments earlier as I can't find a related issue.

Anyway, thank you to all Redmine contributors. This is a great piece of software, and we enjoy using it daily.

#17 - 2013-12-31 14:31 - Pierre Maigne

<wrong manipulation :->

#18 - 2013-12-31 21:12 - Mischa The Evil

- Related to Defect #15789: Users can see all groups when adding a filter "Assignee's Group" added

#19 - 2014-04-15 22:18 - Rafał Lisowski

- File 0001-watchers-fix.patch added

In my opinion, should be visible only users associated with the project.
I don't have any public projects so it is easy choice for me.

#20 - 2014-04-29 12:44 - Pierre Maigne

Thanks Rafał for this new fix, it works like a charm on 2.5.1 !

#21 - 2014-07-29 10:31 - Pierre Maigne

Just a little issue with Rafał patch : if you add watchers to an existing issue, it doesn't refresh the list automatically, you have to refresh the page entirely to update the watcher list. Unfortunately, I'm not a ruby developer and can't figure out why.

I think this feature should be considered as defect, as it is a security issue.

#22 - 2014-09-24 10:22 - Toshi MARUYAMA

- Related to Feature #17747: Private roles added

#23 - 2014-10-20 22:06 - Mischa The Evil

- Related to Patch #18128: Make User profile 404 rendering more consistent (and speed up Users#show API) added

#24 - 2014-10-25 07:39 - Mischa The Evil

- Related to Feature #6015: Private Users added

#25 - 2014-11-11 14:14 - Jean-Philippe Lang

- Status changed from New to Closed

- Target version changed from Candidate for next major release to 3.0.0

- Resolution set to Fixed

r13584 adds a Users visibility setting on role for controlling which users can be seen.
This applies to user profiles, filters and user search when adding watchers.

#26 - 2014-11-16 08:19 - Mischa The Evil

Great to see this is being included in a release.

Just a question: the two cases given by Etienne in #11724#note-11 are not covered by this yet, right?
I can see that his first point is considered out-of-scope of this issue ~~but I think that the second one is in scope ánd could potentially create unexpected results (I haven't been able to test these changes myself actually, so I can't say for sure...)~~.
Edit by Mischa The Evil: this case (*when a user is not tied to a project [anymore], you can't have any visibility policy applicable*) **is** already covered by r13584 implementation (by making the users visibility role option available to/applicable on the build-in anonymous and non-member roles too, see source:/trunk/app/models/principal.rb@13584#L51).

#27 - 2017-07-28 07:42 - Mischa The Evil

- Related to Feature #26555: Hide user information from other users (even if they are all members of the same project) added

Files

0001-watchers-fix.patch	1.41 KB	2014-04-15	Rafał Lisowski