Redmine - Defect #15123
"Add watcher" leaks all active users

2013-10-14 10:11 - Felix Schäfer

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

Description

When adding watchers, all active users of the current installation are visible (on new issues from the get-go, on existing issues you might have to type a few characters to trigger the autocomplete).

All other places in Redmine exposing users go to great lengths to only show users that are "visible" to the current user. Attached is a patch that limits the proposed users in the watcher autocomplete to users that are members of projects visible to the current user.

(This patch was written on behalf of and contributed by Planio)

Related issues:

Related to Redmine - Defect # 9500: Watchers list before and after creation i...	**New**	**2011-10-31**
Related to Redmine - Feature # 5159: Ability to add Non-Member watchers to th...	**Closed**	**2010-03-23**
Duplicates Redmine - Feature # 11724: Prevent users from seeing other users b...	**Closed**	
Duplicated by Redmine - Defect # 15613: 'Add watchers' within the new issue r...	**Closed**	

History

#1 - 2013-10-14 10:21 - Toshi MARUYAMA

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

#2 - 2013-10-14 10:24 - Toshi MARUYAMA

- Related to Feature #5159: Ability to add Non-Member watchers to the watch list added

#3 - 2013-10-14 10:28 - Toshi MARUYAMA

I think this is intended behavior of #5159.

#4 - 2013-10-14 10:33 - Mischa The Evil

This actually is a duplicate of #11724, where #9500 isn't actually tightly related. I'd suggest to keep this issue open because it contains a patch with tests.
Thanks for sharing this!

#5 - 2013-10-14 10:33 - Mischa The Evil

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

#6 - 2013-10-14 10:38 - Felix Schäfer

I had thought about that, and also about private issues (I'm still not 100% sure how those work, but IIRC watchers can see private issues too?), but I still think the current solution can be improved. The user pages for example still go to great lengths to make sure you can only see the user pages of users that have some activity in a project you can see source:/branches/2.3-stable/app/controllers/users_controller.rb#L68, probably to not disclose too

many users.

I'm not really in favor of adding even more permissions, but what about a second permission for adding watchers: Rename the current permission to "Add any user as watcher" and "Add users you can see as watcher" or something similar?

#7 - 2013-10-14 10:41 - Felix Schäfer

Mischa The Evil wrote:

> *I'd suggest to keep this issue open because it contains a patch*

Yes.

> *with tests.*

No.

This currently should rather be considered a working and solid proof of concept, I especially wanted some discussion as to wether this behavior is intended, if it could or should be improved upon or if the Redmine core is happy with the current state and doesn't want to change it.

#8 - 2013-10-20 06:01 - Mischa The Evil

Felix Schäfer wrote:

> *[...] and also about private issues (I'm still not 100% sure how those work, but IIRC watchers can see private issues too?) [...]*

The watcher mechanism is not (and should not) being used for access control. It is used for notification purposes only. See #8488.
(please post to the forum with questions about the current implementation of private issues, I'd be happy to catch you up on the subject ;)

> *but I still think the current solution can be improved.*

I totally agree.

> *The user pages for example still go to great lengths to make sure you can only see the user pages of users that have some activity in a project you can see source:/branches/2.3-stable/app/controllers/users_controller.rb#L68, probably to not disclose too many users.*

Yes, indeed. And I think this good. See r2986 which introduced these checks for #3720 and #4129.

> *I'm not really in favor of adding even more permissions, but what about a second permission for adding watchers: Rename the current permission to "Add any user as watcher" and "Add users you can see as watcher" or something similar?*

That would solve the issue as far as I can see. Considering the nature of the issue I tend to think that it could justify adding such permission.

> *[...] I especially wanted some discussion as to wether this behavior is intended, if it could or should be improved upon or if the Redmine core is happy with the current state and doesn't want to change it.*

As Toshi stated in note-3 it indeed seems the intended behavior as per #5159.
I definitely think it would be good if this is going to be improved. #11724 was filed initially as a defect, which I think this behavior is in the light of r2986.

> *Mischa The Evil wrote:*
>
> > *with tests.*
>
> *No.*

Hmm, I think I was a bit distracted and made a Freudian typo... ;)
{{collapse(Off-topic...)
This is affecting ChiliProject too. See:

- chiliproject:source:/app/views/watchers/_watchers.rhtml@master#L15, which got introduced for CP-issue 800
- CP-issue 1073

}}

#9 - 2013-10-20 17:50 - Jean-Philippe Lang

- Status changed from New to Closed
- Resolution set to Duplicate

I'm closing it in favour of #11724. Please have a look at my note #11724-8.

#10 - 2013-12-06 14:50 - Toshi MARUYAMA

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

#11 - 2013-12-06 14:50 - Toshi MARUYAMA

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

#12 - 2013-12-06 14:51 - Toshi MARUYAMA

- Duplicated by Defect #15613: 'Add watchers' within the new issue reveals all the accounts added

Files

watchers_autocomplete_visible_only.patch	2.13 KB	2013-10-14	Felix Schäfer