Redmine - Defect #37109
Email fields visibility from journal

2022-05-11 16:09 - Martin Valasik

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

Description

We have detected that notification emails can contain custom fields that should not be visible for given user. We have Issue Custom Fields with specific visibility setting (configured within custom field administration).
Notification emails contains two parts with fields information:

- information from journal what have changed. (using details_to_strings helper function)
- full issue overview (using render_email_issue_attributes helper function)

This two function have different implementation.

- render_email_issue_attributes function validates what should be rendered - which fields can be visible for user. This function contains the user within it's parameters.
- details_to_strings function only shows information from journal and does not validate whether fields are visible for given user.

Thus, some users get information that they can not see and may be sensitive.

We are using Redmine 3.4.4, but based on quick check of current source code the issue should be still there.
Environment:

- Redmine version: 3.4.4.stable
- Ruby version: 2.6.0-p0 (2018-12-25) [x86_64-linux]
- Rails version: 4.2.8
- Environment: production
- Database adapter: Mysql2

History

#1 - 2022-05-30 19:13 - Holger Just

- Status changed from New to Needs feedback

In older Redmine versions (that is, all versions < 4.0), Redmine has grouped notification mails based on attributes of the recipients. This resulted in often only few mails being sent to several recipients. One of the attributes to group notification mails was the visibility of issue custom fields. Specifically, we group notification mails for all users who can see the same set of custom fields of the issue using the Issue#each_notification method which is called by the respective Mailer method.

Starting with Redmine 4.0 (specifically with #26791), Redmine sends individual notification mails for each recipient. Here, we don;t group any notifications anymore but perform the visibility check for each recipient (and thus sent mail) individually.

With that being said, in both versions, the recipients should only see custom fields thay are allowed to see in the atttributes list at the top of the notification mail. This is tested and appears to work fine.

Is your description based on an actual observation or just some general code reading? If you can describe an actual case (which we can reproduce based on an empty Redmine) which allows users to receive notification mails containing custom field details they are not allowed to see, we would be happy to further investigate this.

In any case though, please be aware that Redmine 3.4 is not officially supported by the Redmine project anymore (neither with bug fixes nor security updates). As such, I'd strongly recommend to upgrade your Redmine installation to a newer versions. Right now, we support the 4.2.x as well as the 5.0.x branches.