Redmine - Defect #35045

Mail handler bypasses add_issue_notes permission

2021-04-06 18:05 - Holger Just

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Go MAEDA	**% Done:**	0%
Category:	Email receiving	**Estimated time:**	0.00 hour
Target version:	4.0.9		
Resolution:	Fixed	**Affected version:**	

Description

Following #33689, the distinction between the edit_issues permission and add_issue_notes was increased in that the edit permission does not encompass the permission to add notes on its own.

However, it is currently still possible for users with just the edit_issues permission but without the add_issue_notes permission to add notes to issues by "replying" to issue notification emails (if set up on that particular Redmine).

See https://www.redmine.org/projects/redmine/repository/entry/tags/4.1.2/app/models/mail_handler.rb#L228

In general, I believe that the edit_issues permission was originally intended to also encompass the add_issue_notes permission (since it doesn't make much sense to allow people to change any attribute of the issue but not to add notes). Instead, when the add_issue_notes permission was added, I believe it was intended to be given to users so that they can ONLY add notes but not change any other attribute. This detail appears to be interpreted differently later on, resulting in inconsistently applied permissions now.

Related issues:

Related to Redmine - Feature #17599: Allow users to edit issues without addin...	**New**

Associated revisions

Revision 20970 - 2021-04-25 15:02 - Go MAEDA

Mail handler bypasses add_issue_notes permission (#35045).

Patch by Marius BALTEANU.

Revision 20971 - 2021-04-25 15:06 - Go MAEDA

Merged r20970 from trunk to 4.2-stable (#35045).

Revision 20972 - 2021-04-25 15:10 - Go MAEDA

Merged r20970 from trunk to 4.1-stable (#35045).

Revision 20973 - 2021-04-25 15:32 - Go MAEDA

Merged r20970 from trunk to 4.0-stable (#35045).

History

#2 - 2021-04-20 00:27 - Marius BĂLTEANU

From #17599#note-2:

Jean-Philippe Lang wrote:

> The "Add notes" permission lets users add notes without editing the issue. But whenever a user is allowed to edit an issue, he is allowed to add notes by design.

I think we should stick to that decision and if we really think that it's better to change the design, then it should be addressed in a new issue.

#3 - 2021-04-20 11:16 - Holger Just

- Related to Feature #17599: Allow users to edit issues without adding notes. added

#4 - 2021-04-20 11:20 - Holger Just

Thanks for confirming!

In that case, the patch from #33689 should be reverted. The permissions check for add_issue_notes then needs to be updated so that the notes form field is also shown if the user ONLY has the edit_issues permission. #33689 and #17599 should then be changed to closed/wont fix.

#5 - 2021-04-23 00:25 - Marius BĂLTEANU

- Assignee set to Go MAEDA

Go Maeda, #33689 was handled by you, what do you think about this?

#6 - 2021-04-23 10:47 - Go MAEDA

As Holger wrote, it is a problem that users cannot add notes even though you have edit_issue permission.

I think that users who do not have either edit_issue or add_notes permissions should not be able to add notes via API, but I am not against reverting #33689 for now.

#7 - 2021-04-23 12:20 - Holger Just

If we revert the behavior change of #33689, we should at the same time adapt Issue#notes_addable? to bring the UI behavior in line with that of the MailHandler and the API, e.g.

```
def notes_addable(user=User.current)
  user_tracker_permission?(user, :add_issue_notes) || user_tracker_permission?(user, :edit_issues)
end
```

(Note that I have not conclusively tested the above code for now.)

Apart from the changing tests, this should however allow to retain the model change in #33689.

#8 - 2021-04-23 12:23 - Marius BĂLTEANU

I agree with you, Holger. Unfortunately, until Saturday night, I don't have time to work on this.

#9 - 2021-04-25 10:23 - Marius BĂLTEANU

Looking deeper in the code, I've observed that r15466 for #285 changed the existing behaviour and explicit required the add_notes permission to allow users to add notes to an issue. Since then, the add_notes permission is configurable per each tracker (together with view_issues, add_issues, edit_issues and delete_issues) which makes harder to revert to the old behaviour. Also, considering those granular permissions, it is less confusing if we keep them separated without any inheritance.

Considering these new findings, I'm in favour of properly check the permission when the notes are added from email and add #17599 to Changelog.

What do you think?

#10 - 2021-04-25 10:43 - Go MAEDA

Marius BALTEANU wrote:

> Considering these new findings, I'm in favour of properly check the permission when the notes are added from email and add #17599 to Changelog.

It is rather a big change, so it's probably better to apply the change in Redmine 5.0 instead of a minor version. The change may cause some existing instances to suddenly stop updating issues via email.

#11 - 2021-04-25 10:55 - Marius BĂLTEANU

How this change is different with the one from #33689 which was delivered in a minor release? From my point of view, it's the same thing.

I agree with you that this change was big, but considering that it's in the UI since Redmine 3.3.0 and in the API since Redmine 4.0.8, I don't see a real reason to wait for Redmine 5.0.0 to have these permissions consistent.

The patch is the following:

```
--- a/app/models/mail_handler.rb
+++ b/app/models/mail_handler.rb
@@ -225,8 +225,7 @@ class MailHandler < ActionMailer::Base

     # check permission
     unless handler_options[:no_permission_check]
-      unless user.allowed_to?(:add_issue_notes, issue.project) ||
-               user.allowed_to?(:edit_issues, issue.project)
```

```
+       unless issue.notes_addable?
+         raise UnauthorizedAction, "not allowed to add notes on issues to project [#{issue.project.name}]"
+       end
      end
diff --git a/test/unit/mail_handler_test.rb b/test/unit/mail_handler_test.rb
index 836df11d6..3fd3ce072 100644
--- a/test/unit/mail_handler_test.rb
+++ b/test/unit/mail_handler_test.rb
@@ -1051,9 +1051,11 @@ class MailHandlerTest < ActiveSupport::TestCase
     end
   end

-  def test_reply_to_a_issue_without_permission
+  def test_reply_to_an_issue_without_permission
     set_tmp_attachments_directory
-    Role.all.each {|r| r.remove_permission! :add_issue_notes, :edit_issues}
+    # "add_issue_notes" permission is explicit required to allow users to add notes
+    # "edit_issue" permission no longer includes the "add_issue_notes" permission
+    Role.all.each {|r| r.remove_permission! :add_issue_notes}
     assert_no_difference 'Issue.count' do
       assert_no_difference 'Journal.count' do
         assert_not submit_email('ticket_reply_with_status.eml')
(END)
```

#12 - 2021-04-25 10:58 - Jean-Philippe Lang

Marius BALTEANU wrote:

> Also, considering those granular permissions, it is less confusing if we keep them separated without any inheritance.

I agree with this. Even if editing an issue with having the ability to add note may not be very common, it makes it more clear to separate permissions.

#13 - 2021-04-25 12:45 - Marius BĂLTEANU

- Target version set to 4.0.9

#14 - 2021-04-25 14:47 - Go MAEDA

- Subject changed from Inconsistent permissions for issue_edit and add_issue_notes to Mail handler bypasses add_issue_notes permission

#15 - 2021-04-25 15:33 - Go MAEDA

- Status changed from New to Resolved

Committed the change #35045#note-11.

#16 - 2021-04-26 18:19 - Marius BĂLTEANU

- Status changed from Resolved to Closed

#17 - 2021-04-28 10:24 - Holger Just

CVE-2021-31864 has been assigned for this.

#18 - 2022-06-21 08:11 - Marius BĂLTEANU

- Project changed from 2 to Redmine

- Category set to Email receiving

- Resolution set to Fixed