Redmine - Defect #34029

403 Forbidden error when non-member try to upload a file

2020-09-24 10:51 - Vincent Robert

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Marius BĂLTEANU	**% Done:**	100%
Category:	Permissions and roles	**Estimated time:**	0.00 hour
Target version:	5.0.0		
Resolution:	Fixed	**Affected version:**	4.1.1

Description

Hello

Our users encountered an error in a specific case, when uploading files.

Here is a screenshot showing the 403-forbidden error after the upload:

error.png

Steps to reproduce

This error happens in a specific case when the user is not a member of the project.
Here are the steps to reproduce the issue:

- The current user is NOT member of any project
- The build-in role "non-member" has NO permission at all
- In the project's members tab, a role is set for the member "non-member" and this role has permission to create and update issues

Logs

On the server side, here are the logs:

```
Started POST "/uploads.js?attachment_id=1&filename=image-test.jpg&content_type=image%2Fjpeg" for 1
27.0.0.1 at 2020-09-24 10:30:51 +0200
Processing by AttachmentsController#upload as JS
  Parameters: {"attachment_id"=>"1", "filename"=>"image-test.jpg", "content_type"=>"image/jpeg"}
  Token Update All (12.1ms)  UPDATE "tokens" SET "updated_on" = '2020-09-24 10:30:51.312455' WHERE
 "tokens"."user_id" = $1 AND "tokens"."value" = $2 AND "tokens"."action" = $3  [["user_id", 14], [
"value", "7d688080432d1c8ceafbd03811ad81dbf8193f1f"], ["action", "session"]]
   (0.6ms)  SELECT MAX("settings"."updated_on") FROM "settings"
  User Load (0.5ms)  SELECT  "users".* FROM "users" WHERE "users"."type" IN ('User', 'AnonymousUse
r') AND "users"."status" = $1 AND "users"."id" = $2 LIMIT $3  [["status", 1], ["id", 14], ["LIMIT"
, 1]]
  Current user: visitor (id=14)
  Role Load (1.0ms)  SELECT DISTINCT "roles".* FROM "roles" INNER JOIN "member_roles" ON "member_r
oles"."role_id" = "roles"."id" INNER JOIN "members" ON "members"."id" = "member_roles"."member_id"
 INNER JOIN "projects" ON "projects"."id" = "members"."project_id" WHERE (projects.status <> 9) AN
D "members"."user_id" = 14
  Role Load (0.2ms)  SELECT  "roles".* FROM "roles" WHERE "roles"."builtin" = $1 LIMIT $2  [["buil
tin", 1], ["LIMIT", 1]]
Filter chain halted as :authorize_global rendered or redirected
Completed 403 Forbidden in 20ms (ActiveRecord: 14.4ms)
```

Configuration

The bug has been confirmed on the latest Redmine version, with no plugin installed.

```
Environment:
  Redmine version                 4.1.1.stable
  Ruby version                    2.6.6-p146 (2020-03-31) [x86_64-darwin19]
  Rails version                   5.2.4.2
  Environment                     development
  Database adapter                PostgreSQL
  Mailer queue                    ActiveJob::QueueAdapters::AsyncAdapter
  Mailer delivery                 smtp
SCM:
  Subversion                      1.13.0
  Git                             2.24.1
  Filesystem
Redmine plugins:
  no plugin installed
```

Associated revisions

Revision 21502 - 2022-03-27 23:29 - Marius BĂLTEANU

Include roles of built-in "Non member users" and "Anonymous users" members when user is not a member of the project. This fixes #34029.

Revision 21503 - 2022-03-27 23:30 - Marius BĂLTEANU

Add test for #34029.

Patch by Vincent Robert.

History

#1 - 2020-09-24 15:12 - Vincent Robert

- File patch.diff added

- Target version set to 4.1.2

Please find attached a diff file which contains:

- a system test to reproduce the error
- a patch to fix it

Thank you for considering this patch.

```
  def test_create_issue_with_attachment_when_user_is_not_a_member
    set_tmp_attachments_directory

    # Set no permission to non-member role
    non_member_role = Role.where(:builtin => Role::BUILTIN_NON_MEMBER).first
    non_member_role.permissions = []
    non_member_role.save

    # Set role "Reporter" to non-member users on project ecookbook
    membership = Member.find_or_create_by(user_id: Group.non_member.id, project_id: 1)
    membership.roles = [Role.find(3)] # Reporter
    membership.save

    log_user('someone', 'foo')

    issue = new_record(Issue) do
      visit '/projects/ecookbook/issues/new'
      fill_in 'Subject', :with => 'Issue with attachment'
      attach_file 'attachments[dummy][file]', Rails.root.join('test/fixtures/files/testfile.txt')
      fill_in 'attachments[1][description]', :with => 'Some description'
      click_on 'Create'
    end
    assert_equal 1, issue.attachments.count
    assert_equal 'Some description', issue.attachments.first.description
  end
```

```
       # authorize if user has at least one role that has this permission
-      roles = self.roles.to_a | [builtin_role]
+      roles = self.roles.to_a | [builtin_role] | Group.non_member.roles.to_a | Group.anonymous.roles.to_a
       roles.any? {|role|
         role.allowed_to?(action) && ...
```

#2 - 2021-03-15 22:30 - Marius BĂLTEANU

- Target version changed from 4.1.2 to 4.2.0

Moving this to a major version (4.2.0) because the proposed patch moves a method from one class to another.

#3 - 2021-03-25 08:34 - Marius BĂLTEANU

- Target version changed from 4.2.0 to 5.0.0

Need more time to review and fix.

#4 - 2021-11-08 20:46 - Rob Logan

+1

Hand applied the patch to my 4.2.2 system (app/models/user.rb reformatted def roles) and it appears to solve the problem.

#5 - 2022-02-02 19:33 - Dariusz Makowski

I have the same problem. I'm on :

```
Environment:
  Redmine version                4.2.3.stable
  Ruby version                   2.6.9-p207 (2021-11-24) [x86_64-linux]
  Rails version                  5.2.6
  Environment                    production
  Database adapter               Mysql2
  Mailer queue                   ActiveJob::QueueAdapters::AsyncAdapter
  Mailer delivery                smtp
SCM:
  Subversion                     1.14.1
  Git                            2.34.1
  Filesystem
Redmine plugins:
```

I tried to add the tweak to user.rb like Robert Hammer Logan did, but sadly it does not work for me :- (
It actually broke more and I have Internal Error instead now.

Any hints? I want to allow self-registered-authenticated users to attach attachments...

#6 - 2022-03-19 13:39 - Marius BĂLTEANU

Dariusz Makowski wrote:

> I have the same problem. I'm on :
>
> [...]
>
> I tried to add the tweak to user.rb like Robert Hammer Logan did, but sadly it does not work for me :- (
> It actually broke more and I have Internal Error instead now.
>
> Any hints? I want to allow self-registered-authenticated users to attach attachments...

Can you check in the logs what error do you receive?

#7 - 2022-03-20 22:13 - Marius BĂLTEANU

- File 0001-Include-GroupNonMember-and-GroupAnonymous-roles-3402.patch added

Vincent, what do you think about the following fix?

I tried to fix the method User#roles to include the roles assigned to Group Non Member or Group Anonymous Users groups. For example, roles_for_project already do this.

Also, only the roles assigned to public projects are included in the query.

#8 - 2022-03-20 22:15 - Marius BĂLTEANU

- Assignee set to Marius BĂLTEANU

#9 - 2022-03-21 14:41 - Vincent Robert

Hello Marius. Thank you for this update.

About the fix, I think we should cumulate these roles.
A member should never have fewer permissions than a non-member ; a non-member should never have fewer permissions than an anonymous.

As I see it, a member should have all the permissions granted to these roles : member.roles + non_member.roles + anonymous.roles

#10 - 2022-03-21 21:07 - Marius BĂLTEANU

roles_for_project (source:/trunk/app/models/user.rb#L637) doesn't do this, it overrides the roles only if the user is not a member. At the same time, being a global context, I agree that it makes sense to cumulate them or do cumulate the roles from public projects where the user is not a member.

Being a quite important design choice, I would like more feedback.

What do you think if I commit the fix just for this issue for now to catch the next releases and discuss more in a different issue?

#11 - 2022-03-22 07:48 - Go MAEDA

Vincent Robert wrote:

> About the fix, I think we should cumulate these roles.
> A member should never have fewer permissions than a non-member ; a non-member should never have fewer permissions than an anonymous.

I am against the change. I think it is confusing if the set of permissions for a role is different from as configured. And the change may damage the flexibility of permissions and roles.

#12 - 2022-03-22 08:50 - Vincent Robert

It may actually be a different topic. I agree, we can first fix the bug with the 403 error, without modifying current roles' inheritance.

#13 - 2022-03-27 23:30 - Marius BĂLTEANU

- Status changed from New to Closed

- % Done changed from 0 to 100

Applied in changeset r21502.

#14 - 2022-03-27 23:30 - Marius BĂLTEANU

- Resolution set to Fixed

Files

error.png	69.7 KB	2020-09-24	Vincent Robert
patch.diff	2.91 KB	2020-09-24	Vincent Robert
0001-Include-GroupNonMember-and-GroupAnonymous-roles-3402.patch	1.07 KB	2022-03-20	Marius BĂLTEANU