Redmine - Defect #30731

"View differences" buttons are shown in the repository page even without "Browse repository" permission

2019-02-02 03:12 - Go MAEDA

Status:	Closed		**Start date:**	
Priority:	Normal		**Due date:**	
Assignee:	Jean-Philippe Lang		**% Done:**	0%
Category:	SCM		**Estimated time:**	0.00 hour
Target version:	4.0.3			
Resolution:	Fixed		**Affected version:**	

Description

You are not allowed to see the diff between changesets if you don't have a "Browse repository" permission. However, "View differences" buttons on RepositoriesController#show page are always shown even if you don't have the permission. In contrast, the "View differences" tab on the RepositoriesController#revision is hidden depending on the permission.

I think the buttons should be hidden if the current user does not have a "Browse repository" permission.

Associated revisions

Revision 18013 - 2019-03-30 07:13 - Jean-Philippe Lang

"View differences" buttons are shown in the repository page even without "Browse repository" permission (#30731).

Patch by Go MAEDA.

Revision 18017 - 2019-03-30 08:14 - Jean-Philippe Lang

Merged r18013 to 4.0-stable (#30731).

History

#1 - 2019-03-08 05:23 - Takenori TAKAKI

- File fix-30731.patch added

It seems to be able to solve this problem by adding the following condition for disp the button.

```
User.current.allowed_to?(:browse_repository, @repository.project)
```

I made a patch and attached it.

#2 - 2019-03-24 06:31 - Go MAEDA

- Target version set to Candidate for next minor release

Thank you for the patch. While reviewing the patch, I found that we don't have to show radio buttons to select revisions to show diff when "View differences" is hidden.

IMHO, the following fix is better. It hides the radio boxes as well as the button. In addition, it is simpler.

```
diff --git a/app/views/repositories/_revisions.html.erb b/app/views/repositories/_revisions.html.erb
index 914999b34..514380791 100644
--- a/app/views/repositories/_revisions.html.erb
+++ b/app/views/repositories/_revisions.html.erb
@@ -20,7 +20,7 @@ end %>
        :repository_id => @repository.identifier_param, :path => to_path_param(path)},
        :method => :get
      ) do %>
-<% show_diff = revisions.size > 1 %>
+<% show_diff = revisions.size > 1 && User.current.allowed_to?(:browse_repository, @repository.project) %>
 <%= submit_tag(l(:label_view_diff), :name => nil) if show_diff %>
 <table class="list changesets">
 <thead><tr>
```

#3 - 2019-03-25 03:59 - Takenori TAKAKI

Right, As you said the radio button should also be hidden.
I also thought that the proposed patch is simpler and better.

#4 - 2019-03-25 09:34 - Go MAEDA

- File test-for-30731.diff added

- Target version changed from Candidate for next minor release to 4.0.3

Setting the target version to 4.0.3.

#5 - 2019-03-27 01:38 - Go MAEDA

- Subject changed from "View differences" buttons are shown on the repository page even if the user does not have a "Browse repository" permission to "View differences" buttons are shown in the repository page even without "Browse repository" permission

#6 - 2019-03-30 08:14 - Jean-Philippe Lang

- Status changed from New to Closed

- Assignee set to Jean-Philippe Lang

- Resolution set to Fixed

Committed, thanks.

Files

view-diff-button@2x.png	39.4 KB	2019-02-02	Go MAEDA
fix-30731.patch	872 Bytes	2019-03-08	Takenori TAKAKI
test-for-30731.diff	916 Bytes	2019-03-25	Go MAEDA