Redmine - Defect #21136
Issues API may disclose changeset messages that are not visible

2015-11-02 22:44 - Jan from Planio www.plan.io

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	Issues	**Estimated time:**	0.00 hour
Target version:	2.6.8		
Resolution:	Fixed	**Affected version:**	

Description

The check to include related changesets in the single issue API view currently is done against the project of the issue.

An issue can have related changesets from other projects, where the current user might not have the permission to see changesets. This leads to changeset messages being leaked to users without the permission to see those.

The attached patch (created by Felix Schäfer) uses the changesets passed by the controller instead of reimplementing logic in the view, thus sharing the same logic as the html view.

Associated revisions

Revision 14794 - 2015-11-04 19:17 - Jean-Philippe Lang

Fixed that Issues API may disclose changesets that are not visible (#21136).

Revision 14841 - 2015-11-08 10:05 - Jean-Philippe Lang

Merged r14794 (#21136).

Revision 14842 - 2015-11-08 10:06 - Jean-Philippe Lang

Merged r14794 (#21136).

Revision 14843 - 2015-11-08 10:09 - Jean-Philippe Lang

Merged r14794 (#21136).

History

#1 - 2015-11-04 19:19 - Jean-Philippe Lang

- Status changed from New to Resolved

- Assignee set to Jean-Philippe Lang

- Resolution set to Fixed

Thanks for reporting this. The fix is committed in r14794.

The :repositories fixtures were missing in the test, and adding them made the test fail (the user used in the test had actually access to the changeset).

#2 - 2015-11-04 20:08 - Jan from Planio www.plan.io

Jean-Philippe Lang wrote:

> *The :repositories fixtures were missing in the test, and adding them made the test fail (the user used in the test had actually access to the changeset).*

Thanks for committing this (and for pointing this out as well).

#3 - 2015-11-08 10:10 - Jean-Philippe Lang

- Project changed from Security to Redmine

- Subject changed from Information leak in IssuesController#show API to Issues API may disclose changeset messages that are not visible

- Category set to Issues

- Status changed from Resolved to Closed

- Target version set to 2.6.8

- Private changed from No to Yes

#4 - 2015-11-27 08:49 - Jan from Planio www.plan.io

- Private changed from Yes to No

Making this public since fixes have been released already.

Files

231789.patch	3.16 KB	2015-11-02	Jan from Planio www.plan.io