Redmine - Patch #27676
Information leak on roadmap and versions view

2017-11-29 17:27 - Jan from Planio www.plan.io

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	Roadmap	**Estimated time:**	0.00 hour
Target version:	4.0.0		

Description

When limiting a role's permission to only access "Issues created by or assigned to the user", the roadmap (/projects/:identifier/roadmap) and version details (versions/:id) view leaks information about inaccessible issues and time estimations. Due to missing permission checks in Version#fixed_issues the restricted user may see the overall number of issues, their status, tracker, author, category, and time estimations.

We think, this a security-relevant information leak and it should be fixed and announced responsibly. Attached you may find a proposed patch which includes tests and a fix.

The attached patch changes the Version model, so that the calculation methods (closed_issues_count, open_issues_count, etc) are now also available on the fixed_issues relation proxy object. In a second step, all relevant places, where those calcuation methods are used, are updated to include the visible scope. This fixes the roadmap view, the version details view and the version summary in the Gantt chart.

This bug was reported by a Planio user, the patch series was developed by Gregor Schmidt.

Related issues:

Related to Redmine - Defect # 15258: Roadmap Issue Count off	**Closed**
Duplicated by Redmine - Defect # 19187: Roadmap links in subproject	**Closed**
Duplicated by Redmine - Defect # 19059: Wrong number of issues for a version ...	**Closed**

Associated revisions

Revision 17050 - 2017-11-29 20:36 - Jean-Philippe Lang

Moves issue calculations into the fixed_issues relation (#27676).

This way, we can reuse them on refined relations,
e.g. version.fixed_issues.closed_count vs. version.fixed_issues.visible.closed_count

Patch by Gregor Schmidt.

Revision 17051 - 2017-11-29 20:37 - Jean-Philippe Lang

Adds visibility checks on version views (#27676).

Previously not all data on the roadmap and version view where properly
checked against the issue visibility setting. Unprivileged users were
able to see the total number of issues, their estimations and the
open/close status - even if the user was only allowed to see their own issues.

Patch by Gregor Schmidt.

Revision 17052 - 2017-11-29 20:38 - Jean-Philippe Lang

Performance opt - cache AR Proxy for Version#fixed_issues.visible (#27676).

Patch by Gregor Schmidt.

Revision 17053 - 2017-11-29 20:38 - Jean-Philippe Lang

Fixes visibility checks for version.fixed_issues in Gantt (#27676).

Like the version page - the Gantt chart featured a "percent done" info
for each version, which wasn't properly limited to visible issues.

Patch by Gregor Schmidt.

Revision 17251 - 2018-04-01 04:16 - Go MAEDA

Add a test to ensure that issue calculations on version details page take into account only visible issues (#27676).

Patch by Marius BALTEANU.

History

#1 - 2017-11-29 20:54 - Jean-Philippe Lang

I've committed the patch serie, thanks.

This issue was already reported long time ago and it was chosen not to change the behaviour (see #15258). With this change, different users might now see different progress values for the same version and this can be confusing. I think we should add a message for when there are issues assigned to the version that are not visible to the user, for example:

- When all issues are visible: no change
- When there are no visible issues but other issues exist: "No visible issues for this version" (instead of "No issues for this version")
- When there are visible issues and other issues exist: "Some issues assigned to this version are not visible and not taken into account" (message added)
- When there are no issues: no change ("No issues for this version")

What do you think? IMO, it's important to let the user know that are other (not visible) issues that are assigned to the version.

#2 - 2017-11-29 20:56 - Jean-Philippe Lang

- Related to Defect #15258: Roadmap Issue Count off added

#3 - 2017-11-29 20:58 - Jean-Philippe Lang

Also reported in #9411 and #15248

#4 - 2017-12-19 15:12 - Jan from Planio www.plan.io

Thank you for your feedback. Here's what Gregor said:

> *I agree. It may be confusing, that two users may see different roadmaps. On the other hand, the same is true for issue lists, Gantt charts and many other views. This would be the first place, where a special note about invisible elements is added. It feels like a paradigm shift to me.*
>
> *I don't want to argue against that change. I merely want to be sure, that it's done without proper thought.*

#5 - 2017-12-30 18:05 - Toshi MARUYAMA

How about #19187 and #19059?
Marius provides test case in #19187#note-4.

#6 - 2018-03-31 10:25 - Go MAEDA

- Target version set to 4.0.0

This issue should appear in the changelog. Setting target version to 4.0.0.

#7 - 2018-04-01 04:25 - Go MAEDA

- Duplicated by Defect #19187: Roadmap links in subproject added

#8 - 2018-04-02 00:22 - Go MAEDA

- Duplicated by Defect #19059: Wrong number of issues for a version in the roadmap added

#9 - 2018-09-23 15:35 - Jean-Philippe Lang

- Status changed from New to Closed
- Assignee set to Jean-Philippe Lang

#10 - 2018-12-09 07:34 - Jean-Philippe Lang

- Project changed from Security to Redmine
- Category set to Roadmap

Files

0004-Fixes-visibility-checks-for-version.fixed_issues-in-.patch	3.11 KB	2017-11-29	Jan from Planio www.plan.io
0002-Adds-visibility-checks-on-version-views.patch	4.93 KB	2017-11-29	Jan from Planio www.plan.io
0003-Performance-opt-cache-AR-Proxy-for-Version-fixed_iss.patch	5.93 KB	2017-11-29	Jan from Planio www.plan.io
0001-Moves-issue-calculations-into-the-fixed_issues-relat.patch	7.17 KB	2017-11-29	Jan from Planio www.plan.io