

## Redmine - Defect #37171

### Ability to change the issue category or issue target version with nonexistent value for the specific project

2022-05-29 23:01 - Nikola Milanov

<b>Status:</b>	Closed	<b>Start date:</b>	
<b>Priority:</b>	High	<b>Due date:</b>	
<b>Assignee:</b>	Marius BALTEANU	<b>% Done:</b>	0%
<b>Category:</b>	Security	<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>	4.2.7	<b>Affected version:</b>	4.2.5
<b>Resolution:</b>	Fixed		
<b>Description</b>			
<p>Hi there,</p> <p>I found a way to change category with nonexistent ID for the specific project.</p> <p>I will try to explain it in more details (the user making the change has access to the project)</p> <ol style="list-style-type: none"><li>1. User start editing the ticket (click "Edit" button)</li><li>2. Right click on Category field and choose "Inspect" (Developer's tool)</li><li>3. Then we change the value of the category to one that is not in the project</li><li>4. Click "Submit" button and we save the ID of category that not exist for the specific folder.</li></ol> <p>Is there any way to make to verify that this category is in the project to avoid this kind of changes?</p> <p>Cheers</p>			

#### Associated revisions

---

##### Revision 21637 - 2022-06-16 17:10 - Marius BALTEANU

Ensure category\_id is valid within the issue's project (#37171).

Patch by Holger Just.

##### Revision 21638 - 2022-06-16 17:13 - Marius BALTEANU

Improved fixed\_version\_id validation (#37171).

Patch by Holger Just.

##### Revision 21639 - 2022-06-16 23:28 - Marius BALTEANU

Merged r21637 and r21638 to 5.0-stable (#37171).

##### Revision 21640 - 2022-06-16 23:29 - Marius BALTEANU

Merged r21637 and r21638 to 4.2-stable (#37171).

#### History

---

##### #1 - 2022-05-30 03:40 - Mischa The Evil

- Subject changed from *Ability to change the category with nonexistent for the specific project* to *Ability to change the issue category with nonexistent value for the specific project*
- Category changed from *Issues* to *Security*
- Status changed from *New* to *Confirmed*
- Priority changed from *Normal* to *High*
- Private changed from *No* to *Yes*

@Nikola Milanov: Thanks for reporting this issue.

I was able to reproduce the reported behavior using the provided steps on an old 4.2-stable (Rails 5.x) playground. I think this affects current trunk (Rails 6.x) too, but I haven't actually tested this.

I currently don't know for sure how pervasive this behavior is in that it might extend to other fields and/or modules, but this should nevertheless be properly investigated and acted upon given the potential security implications of this issue (issue and (custom) field visibility, workflows, assignees, API-request behavior, etc.).

Given all the above I'll:

- set the issue to private;
- set the issue priority to High;
- set the issue category to Security; and
- add Go, Holger and Marius as watchers.

@Go, @Holger, @Marius: Can you'll have a look into this matter?

#### **#2 - 2022-05-30 13:16 - Holger Just**

- Assignee set to *Holger Just*

I'll have a look later today.

#### **#3 - 2022-05-30 18:54 - Holger Just**

- File *0001-Validate-category\_id-against-available-categories-in.patch* added
- File *0002-Validate-fixed\_version\_id-to-ensure-that-a-version-w.patch* added
- Assignee changed from *Holger Just* to *Marius BALTEANU*

Attached, there are two patches to improve the validations:

- *0001-Validate-category\_id-against-available-categories-in.patch* added the validation for the `category_id` to ensure that the given category is valid within the issue's project.
- *0002-Validate-fixed\_version\_id-to-ensure-that-a-version-w.patch* improves the validation of the `fixed_version_id` to ensure that no invalid version (that is: one that does not exist at all) can be given.

I think all of the other fields are fine since they either reference global data (`project`, `tracker`, `assigned_to`, `author`, `status`) and/or are correctly checked already.

Marius or Maeda-san, could either of you check those patches and merge them? They should cleanly apply to the current trunk, 5.0-stable and 4.2-stable. I'm assigning the issue to Marius, please feel free to re-assign as necessary.

#### **#4 - 2022-06-16 17:13 - Marius BALTEANU**

- Status changed from Confirmed to Resolved
- Target version set to 4.2.7
- Resolution set to Fixed

Thanks, I've committed both patches and I'm going to merge them to the stable branches once the tests pass.

**#5 - 2022-06-16 23:29 - Marius BALTEANU**

- Subject changed from Ability to change the issue category with nonexistent value for the specific project to Ability to change the issue category or issue target version with nonexistent value for the specific project
- Status changed from Resolved to Closed

Merged to stable branches.

**#6 - 2022-06-21 08:09 - Marius BALTEANU**

- Private changed from Yes to No

**Files**

---

0002-Validate-fixed_version_id-to-ensure-that-a-version-w.patch	1.87 KB	2022-05-30	Holger Just
0001-Validate-category_id-against-available-categories-in.patch	1.66 KB	2022-05-30	Holger Just