Redmine - Defect #33417

Updating an issue via REST API causes internal server error if invalid project id is specified

2020-05-08 09:44 - Fredrik Fornwall

Status:	Closed		**Start date:**	
Priority:	Normal		**Due date:**	
Assignee:	Go MAEDA		**% Done:**	0%
Category:	REST API		**Estimated time:**	0.00 hour
Target version:	4.1.2			
Resolution:	Fixed		**Affected version:**	

Description

Hello!

With a redmine instance up and running at http://localhost:3000, the following request (in https://requests.readthedocs.io/en/master/ syntax, but can be easily translated to other request formats):

```
requests.post('http://user:password@localhost:3000/issues.xml', json={'issue': {'project_id': 0, 'status_id': '', 'tracker_id': 0, 'assigned_to_id': '0'}})
```

results in a 500 Internal Server Error:

```
NoMethodError (undefined method `assignable_users' for nil:NilClass):

app/models/issue.rb:941:in `assignable_users'
app/models/issue.rb:742:in `validate_issue'
app/controllers/issues_controller.rb:143:in `create'
lib/redmine/sudo_mode.rb:64:in `sudo_mode'
```

This issue was found while trying out https://meeshkan.com, our tool under development to automatically scan API using projects for issues, on open source repositories. Feel free to install the Meeshkan github app on https://github.com/redmine/redmine if you are interested in getting more reports from our scans in the future!

Associated revisions

Revision 19777 - 2020-05-14 16:33 - Go MAEDA

Updating an issue via REST API causes internal server error if invalid project id is specified (#33417).

Patch by Go MAEDA.

Revision 19779 - 2020-05-16 01:16 - Go MAEDA

Merged r19777 from trunk to 4.1-stable (#33417).

History

#1 - 2020-05-08 11:33 - Go MAEDA

- Category set to REST API

- Status changed from New to Confirmed

I have confirmed that the reported exception is raised when an invalid project id is given.

#2 - 2020-05-09 04:31 - Go MAEDA

"POST /issues.(json|xml)" raises exception when the following parameters are given:

1. *Any value* for assigned_to_id and an *invalid value* for project_id.

```
{"issue": {"project_id": 0, "assigned_to_id": "1"}}
```

2. *Any value* for fixed_version_id and an *invalid value* for project_id.

```
{"issue": {"project_id": 0, "fixed_version_id": "1"}}
```

Here is a workaround for this issue:

```
diff --git a/app/models/issue.rb b/app/models/issue.rb
index 487b1b552..e665a46cb 100644
--- a/app/models/issue.rb
+++ b/app/models/issue.rb
@@ -723,7 +723,7 @@ class Issue < ActiveRecord::Base
         errors.add :start_date, :earlier_than_minimum_start_date, :date => format_date(soonest_start)
       end

-    if fixed_version
+    if project && fixed_version
       if !assignable_versions.include?(fixed_version)
         errors.add :fixed_version_id, :inclusion
       elsif reopening? && fixed_version.closed?
@@ -738,7 +738,7 @@ class Issue < ActiveRecord::Base
         end
       end

-    if assigned_to_id_changed? && assigned_to_id.present?
+    if project && assigned_to_id_changed? && assigned_to_id.present?
       unless assignable_users.include?(assigned_to)
         errors.add :assigned_to_id, :invalid
       end
@@ -938,6 +938,8 @@ class Issue < ActiveRecord::Base

   # Users the issue can be assigned to
   def assignable_users
+    return [] if project.nil?
+
     users = project.assignable_users(tracker).to_a
     users << author if author && author.active?
     if assigned_to_id_was.present? && assignee = Principal.find_by_id(assigned_to_id_was)
@@ -949,6 +951,7 @@ class Issue < ActiveRecord::Base
   # Versions that the issue can be assigned to
   def assignable_versions
     return @assignable_versions if @assignable_versions
+    return [] if project.nil?

     versions = project.shared_versions.open.to_a
     if fixed_version
```

#3 - 2020-05-09 08:35 - Go MAEDA

- File 33417.patch added

- Target version set to Candidate for next minor release

Attaching a patch with tests.

#4 - 2020-05-12 11:57 - Go MAEDA

- Target version changed from Candidate for next minor release to 4.1.2

Setting the target version to 4.1.2.

#5 - 2020-05-14 16:33 - Go MAEDA

- Subject changed from Internal Server Error in POST to /issues.xml to Updating an issue via REST API causes internal server error if invalid project id is specified

- Status changed from Confirmed to Resolved

- Assignee set to Go MAEDA

- Resolution set to Fixed

Committed the patch. Thank you for reporting the issue.

#6 - 2020-05-16 01:17 - Go MAEDA

- Status changed from Resolved to Closed

Files