Redmine - Defect #37719

Broken serialized columns, if saved time was with Rails 4.2

2022-09-28 05:16 - Alexander Meindl

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

Description

Broken serialized columns, if saved time was with Rails 4.2

All serialized columns are broken, if the data in database was saved with Rails 4.2 in older redmine versions.

This bug was introducted with #37452 and CVE-2022-32224

E.g. saved settings for all plugins are broken, if the last save was with Rails 4.2:

```
Psych::DisallowedClass (Tried to load unspecified class: ActionController::Parameters):

app/models/setting.rb:111:in `value'
app/models/setting.rb:125:in `[]'
app/models/setting.rb:320:in `plugin_redmine_issue_templates'
app/controllers/settings_controller.rb:78:in `plugin'
lib/redmine/sudo_mode.rb:61:in `sudo_mode'
```

The easiest solution for this would be, to add "ActionController::Parameters" to config.active_record.yaml_column_permitted_classes
Maybe there is an other solution to convert ActionController::Parameters to ActiveSupport::HashWithIndifferentAccess for existing stored data, but I did not found one.

I think it is important to solve this bug before releasing 5.0.3, because lots of Redmine systems are affected by this problem.

My environment:

- Redmine Master (same bug with upcoming 5.0.3)
- PostgreSQL 14
- Ruby 3.1.2 (same problem with older ruby versions)

Related issues:

Related to Redmine - Patch #37452: Update Rails to 6.1.7	**Closed**
Related to Redmine - Patch #37465: Update Rails to 5.2.8.1	**Closed**

Associated revisions

Revision 21863 - 2022-09-28 08:36 - Go MAEDA

Fix Psych::DisallowedClass exception when loading plugin settings saved with Rails 4.2 (#37452, #37719).

Patch by Alexander Meindl.

Revision 21864 - 2022-09-28 08:37 - Go MAEDA

Merged r21863 from trunk to 5.0-stable (#37452, #37719).

Revision 21871 - 2022-09-30 09:01 - Go MAEDA

Merged r21863 from trunk to 4.2-stable (#37465, #37719).

History

#1 - 2022-09-28 06:53 - Go MAEDA

Could you tell me the version of Redmine and Issue Templates Plugin?

I tried to reproduce the issue by migrating the database from the following environment to the current trunk but I could not.

Source environment: Redmine 3.4.13 (Rails 4.2.11.1), Redmine Issue Templates Plugin 0.2.1

#2 - 2022-09-28 07:13 - Alexander Meindl

Hi,

Did you press "Save" on plugin settings of Issue Templates Plugin?

With "Save" rails stores "ActionController::Parameters" in database (serialize). "Issue Templates Plugin" is only an example, this happens with all serialized columns, which stored data in database with Rails < 5.

I get this error with all plugins, this was just an example. If you update settings with Redmine 5.0.2, data in database uses ActiveSupport::HashWithIndifferentAccess and the problem would be fixed. But with current master, older serialized data with "ActionController::Parameters" could not read anymore because of Psych::DisallowedClass after updating to latest Redmine version.

PS: after update to latest Redmine I use the latest Issue Templates Plugin. I do not remember, which version was active on old redmine version - but I think it doesn't matter, problem exists with all versions.

#3 - 2022-09-28 07:24 - Alexander Meindl

Hi again,

I found some infos to this problem on https://www.redmineup.com/pages/help/troubleshooting/psych-disallowed-class-fix, too.

Btw. not only settings are affected, but any serialized columns.

#4 - 2022-09-28 07:27 - Go MAEDA

- Related to Patch #37452: Update Rails to 6.1.7 added

#5 - 2022-09-28 07:28 - Go MAEDA

- Category set to Plugin API

- Target version set to 4.2.8

Thank you for providing additional information.

Setting the target version to 5.0.3.

#6 - 2022-09-28 07:30 - Go MAEDA

- Target version changed from 4.2.8 to 5.0.3

#7 - 2022-09-28 08:38 - Go MAEDA

- Status changed from New to Closed

- Assignee set to Go MAEDA

- Target version deleted (5.0.3)

Committed the fix as a part of #37452. Thank you for your contribution.

#8 - 2022-09-30 08:31 - Vincent Robert

Can you please apply this fix to the 4.2-stable branch?
This way the bug can be fixed in next release 4.2.8. Thank you.

#9 - 2022-09-30 09:00 - Go MAEDA

- Related to Patch #37465: Update Rails to 5.2.8.1 added

#10 - 2022-09-30 09:02 - Go MAEDA

Vincent Robert wrote:

> Can you please apply this fix to the 4.2-stable branch?
> This way the bug can be fixed in next release 4.2.8. Thank you.

Done in r21871. Thank you for pointing it out.

Files

yaml_column_permitted_classes.patch	527 Bytes	2022-09-28	Alexander Meindl