Redmine - Defect #37814

Plugins that serialize Date or Time objects cause Psych::DisallowedClass exception

2022-10-22 19:25 - Alex Overchenko

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Go MAEDA	**% Done:**	0%
Category:	Rails support	**Estimated time:**	0.00 hour
Target version:	4.2.9		
Resolution:	Fixed	**Affected version:**	4.2.8

Description

I'm upgrading Redmine 4.2.7 to 4.2.8 (docker images) and cannot view any page after user login was done on website.

Upgraded web UI renders that for me:

```
Internal error

An error occurred on the page you were trying to access.
If you continue to experience problems please contact your Redmine administrator for assistance.

If you are the Redmine administrator, check your log files for details about the error.

Back
```

Docker logs:

```
redmine_1  | I, [2022-10-22T17:11:52.640849 #1]  INFO -- : Processing by WelcomeController#index a
s HTML
redmine_1  | I, [2022-10-22T17:11:52.659002 #1]  INFO -- :   Current user: XXX (id=YY)
redmine_1  | I, [2022-10-22T17:11:52.687604 #1]  INFO -- :   Rendering welcome/index.html.erb with
in layouts/base
redmine_1  | I, [2022-10-22T17:11:52.712666 #1]  INFO -- :   Rendered collection of news/_news.htm
l.erb [5 times] (22.0ms)
redmine_1  | I, [2022-10-22T17:11:52.716957 #1]  INFO -- :   Rendered welcome/index.html.erb withi
n layouts/base (29.2ms)
redmine_1  | I, [2022-10-22T17:11:52.719162 #1]  INFO -- : Completed 500 Internal Server Error in
78ms (ActiveRecord: 21.9ms)
redmine_1  | F, [2022-10-22T17:11:52.719874 #1] FATAL -- :
redmine_1  | F, [2022-10-22T17:11:52.719920 #1] FATAL -- : ActionView::Template::Error (Tried to l
oad unspecified class: Date):
redmine_1  | F, [2022-10-22T17:11:52.720092 #1] FATAL -- :     11: <%= favicon %>
redmine_1  |     12: <%= stylesheet_link_tag 'jquery/jquery-ui-1.13.2', 'tribute-5.1.3', 'applicat
ion', 'responsive', :media => 'all' %>
redmine_1  |     13: <%= stylesheet_link_tag 'rtl', :media => 'all' if l(:direction) == 'rtl' %>
redmine_1  |     14: <%= javascript_heads %>
redmine_1  |     15: <%= heads_for_theme %>
redmine_1  |     16: <%= heads_for_auto_complete(@project) %>
redmine_1  |     17: <%= call_hook :view_layouts_base_html_head %>
redmine_1  | F, [2022-10-22T17:11:52.720259 #1] FATAL -- :
redmine_1  | F, [2022-10-22T17:11:52.720405 #1] FATAL -- : app/models/user_preference.rb:69:in `[]
'
redmine_1  | app/models/user_preference.rb:87:in `warn_on_leaving_unsaved'
redmine_1  | app/helpers/application_helper.rb:1713:in `javascript_heads'
redmine_1  | app/views/layouts/base.html.erb:14:in `_app_views_layouts_base_html_erb__593409969835
306285_78780'
redmine_1  | lib/redmine/sudo_mode.rb:61:in `sudo_mode'
```

I'm using MySQL 5.7 as a database.

I have no installed plugins.

I reproduce that error on default configuration: block mapping my configuration to container.

Migrations were redone manually, as described redmineupgrade (https://www.redmine.org/projects/redmine/wiki/Redmineupgrade), step 4 & 5

Now I rolled back to 4.2.7 version, but it looks like I cannot receive any upgrade. That sounds bad.

Associated revisions

Revision 21923 - 2022-10-26 16:04 - Go MAEDA

Add Date and Time classes to yaml_column_permitted_classes (#37814).

Patch by Felix Schäfer.

Revision 21924 - 2022-10-27 03:34 - Go MAEDA

Merged r21923 from trunk to 5.0-stable (#37814).

Revision 21925 - 2022-10-27 03:35 - Go MAEDA

Merged r21923 from trunk to 4.2-stable (#37814).

History

#1 - 2022-10-22 19:33 - Alex Overchenko

Also, some more notes:

- I'm using official docker images: https://hub.docker.com/_/redmine
- I migrated local instance to 5.0.2 version - and all work nice. After upgrading to the latest 5.0.3 I have the same error, as described
- I'm opening root site page for bug reproducing: http://localhost:3000/

#2 - 2022-10-24 08:38 - Go MAEDA

Could you try adding "Date" to yaml_column_permitted_classes in config/application.rb as follows and see if it solves the problem?

```
diff --git a/config/application.rb b/config/application.rb
index 1b22feb12..82a0e18ca 100644
--- a/config/application.rb
+++ b/config/application.rb
@@ -34,6 +34,7 @@ module RedmineApp
     config.active_record.default_timezone = :local
     config.active_record.yaml_column_permitted_classes = [
       Symbol,
+      Date,
       ActiveSupport::HashWithIndifferentAccess,
       ActionController::Parameters
     ]
```

#3 - 2022-10-25 18:45 - Alex Overchenko

Go MAEDA wrote:

> Could you try adding "Date" to yaml_column_permitted_classes in config/application.rb as follows and see if it solves the problem?
>
> [...]

Thanks, Go MAEDA

That manual changes helps to start 4.2.8 & 5.0.3 versions.

Is that changes will be available in 5.0.4, 4.2.9 & next versions?

With regards,
Alex

#4 - 2022-10-25 19:09 - Felix Schäfer

We (Planio) have also observed this with certain plugins and certain of our internal additions saving Date or Time objects in serialised fields such as Settings and UserPreferences, plugin settings and so on.

We would propose adding the Date and Time classes to the list of permitted classes. Those classes were shown in the examples for the mitigation of CVE-2022-32224 and are permitted by default in the safe_yaml gem. They are also integral parts of the standard yaml capabilities and not "added" as tags or any other yaml extension.

```
diff --git a/config/application.rb b/config/application.rb
```

```
index 1b22feb12e..5e93df122d 100644
--- a/config/application.rb
+++ b/config/application.rb
@@ -33,6 +33,8 @@ module RedmineApp
     config.active_record.store_full_sti_class = true
     config.active_record.default_timezone = :local
     config.active_record.yaml_column_permitted_classes = [
+      Date,
+      Time,
       Symbol,
       ActiveSupport::HashWithIndifferentAccess,
       ActionController::Parameters
```

#5 - 2022-10-26 01:59 - Go MAEDA

- Subject changed from Redmine Internal error 500 to Plugins that serialize Date or Time objects cause Psych::DisallowedClass exception

- Category set to Rails support

- Target version set to 4.2.9

Felix Schäfer wrote:

> We would propose adding the Date and Time classes to the list of permitted classes. Those classes were shown in the examples for the mitigation of CVE-2022-32224 and are permitted by default in the safe_yaml gem. They are also integral parts of the standard yaml capabilities and not "added" as tags or any other yaml extension.
>
> [...]

Thank you for suggesting the change. Setting the target version to 4.2.9.

#6 - 2022-10-27 03:38 - Go MAEDA

- Status changed from New to Closed

- Assignee set to Go MAEDA

- Resolution set to Fixed

Committed the fix suggested in #37814#note-4.

Alex Overchenko wrote:

> That manual changes helps to start 4.2.8 & 5.0.3 versions.
>
> Is that changes will be available in 5.0.4, 4.2.9 & next versions?

Yes. See r21924 and r21925.

Files

Screenshot from 2022-10-22 20-21-17.png	19.2 KB	2022-10-22	Alex Overchenko