Redmine - Feature #34062

Upgrade Rails to 5.2.4.5

2020-10-02 09:02 - Daniel Müller

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

Description

CVE-2020-8165 (https://nvd.nist.gov/vuln/detail/CVE-2020-8165)

It would be very helpful if Redmine would work with the latest versions of Ruby and Rails. My server has been shut down for testing, since older versions are in use.

Related issues:

Is duplicate of Redmine - Feature #33906: Upgrade Rails to 5.2.4.5	**Closed**

Associated revisions

Revision 20109 - 2020-10-02 18:32 - Jean-Philippe Lang

Upgrade Rails to 5.2.4.4 (#34062).

Revision 20792 - 2021-03-15 14:38 - Go MAEDA

Merged r20109 from trunk to 4.1-stable (#34062).

Revision 20796 - 2021-03-15 15:36 - Go MAEDA

Merged r20109 from trunk to 4.0-stable (#34062).

History

#1 - 2020-10-02 09:05 - Daniel Müller

https://www.redmine.org/projects/redmine/repository/entry/trunk/Gemfile

```
ruby '>= 2.3.0', '< 2.7.0'
gem 'bundler', '>= 1.12.0'

gem 'rails', '5.2.4.2'
```

At least rails 5.2.4.3 is required! Ruby 2.7 would be helpful, too.

#2 - 2020-10-02 16:15 - Pavel Rosický

I don't think that the current Redmine version is really vulnerable to CVE-2020-8165 because there's no such code (unless you have plugins or modifications), see https://groups.google.com/g/rubyonrails-security/c/bv6fW4S0Y1c

but I'm not so sure for instance about this https://groups.google.com/g/rubyonrails-security/c/NOjKiGeXUgw

note that those vulnerablities were disclosed and fixes are available for 6 months. The fix is 1 line of code. It's sad that there's no reaction from Redmine's team for such a long time :-(

#3 - 2020-10-04 18:31 - Marius BĂLTEANU

- Tracker changed from Defect to Patch

- Subject changed from Security hole in rails to Upgrade Rails to 5.2.4.4

- Assignee set to Jean-Philippe Lang

- Target version set to 4.0.8

#4 - 2020-10-05 08:55 - Daniel Müller

It would be helpful to process security fixes in all current branches like version 4.1.x (https://www.redmine.org/projects/redmine/repository/raw/branches/4.1-stable/Gemfile) and 4.0.x (

https://www.redmine.org/projects/redmine/repository/raw/branches/4.0-stable/Gemfile) not only in trunk.

#5 - 2020-10-05 09:05 - Marius BĂLTEANU

Daniel Müller wrote:

> It would be helpful to process security fixes in all current branches like version 4.1.x (https://www.redmine.org/projects/redmine/repository/raw/branches/4.1-stable/Gemfile) and 4.0.x (https://www.redmine.org/projects/redmine/repository/raw/branches/4.0-stable/Gemfile) not only in trunk.

The stable branches will be updated for sure in the following days.

#6 - 2020-11-01 14:43 - Michael Gerz

This security issue is rated as "critical" (9.8).

When will we see a new Redmnine release to address this issue?

#7 - 2020-11-01 14:52 - Michael Gerz

Note: There are tools out there that check for CVE-2020-8165. Expect more user comments in the near future.

#8 - 2020-12-06 17:33 - Michael Gerz

Just wondering - will this security issue be fixed anytime soon?

#9 - 2020-12-14 08:16 - Mischa The Evil

- Blocked by Feature #33906: Upgrade Rails to 5.2.4.5 added

#10 - 2020-12-16 08:15 - Marius BĂLTEANU

Michael Gerz wrote:

> Just wondering - will this security issue be fixed anytime soon?

Yes, I'm confident that new maintainance releases will be made until end of the year.

#11 - 2021-01-03 00:00 - Michael Gerz

Marius BALTEANU wrote:

> Michael Gerz wrote:
>
> > Just wondering - will this security issue be fixed anytime soon?
>
> Yes, I'm confident that new maintainance releases will be made until end of the year.

Well... then they will be made until the end of 2021. (Anyway... Happy new year!)

#12 - 2021-03-08 10:13 - Markus Boremski

Should we change the Target-Version?
Is 4.0.8 still a real candidate for a release?

#13 - 2021-03-08 13:13 - Michael Gerz

Markus Boremski wrote:

> Should we change the Target-Version?
> Is 4.0.8 still a real candidate for a release?

Well.. the question is: will we see any maintenance release anytime soon?

I far as I can see, there has been only one developer actively committing changes to the source repository in the past 2 1/2 months.

Looks like Redmine is dying slowly.

#14 - 2021-03-15 08:29 - Marius BĂLTEANU

- Subject changed from Upgrade Rails to 5.2.4.4 to Upgrade Rails to 5.2.4.5

- Assignee changed from Jean-Philippe Lang to Go MAEDA

#15 - 2021-03-15 17:06 - Marius BĂLTEANU

- Tracker changed from Patch to Feature

- Status changed from New to Closed

- Target version deleted (4.0.8)

- Resolution set to Duplicate

Rails was upgraded to 5.2.4.5 in #33906.

We'll do our best to release the new maintenance versions this weekend (21-03-2021).

#16 - 2021-03-15 17:06 - Marius BĂLTEANU

- Blocked by deleted (Feature #33906: Upgrade Rails to 5.2.4.5)

#17 - 2021-03-15 17:06 - Marius BĂLTEANU

- Is duplicate of Feature #33906: Upgrade Rails to 5.2.4.5 added