Redmine - Feature #33906

Upgrade Rails to 5.2.4.5

2020-08-26 01:05 - Mischa The Evil

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Go MAEDA	**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	4.0.8		
Resolution:	Fixed		

Description

As released on May 18, 2020 with the following announcement:

> Hi everyone! Rails 5.2.4.3 and 6.0.3.1 have been released! These releases contain important security fixes, so please upgrade when you can.
>
> Both releases contain the following fixes:
>
> [CVE-2020-8162] Circumvention of file size limits in ActiveStorage
> [CVE-2020-8164] Possible Strong Parameters Bypass in ActionPack
> [CVE-2020-8165] Potentially unintended unmarshalling of user-provided objects in MemCacheStore and RedisCacheStore
> [CVE-2020-8166] Ability to forge per-form CSRF tokens given a global CSRF token
> [CVE-2020-8167] CSRF Vulnerability in rails-ujs

Note: the fix for CVE-2020-8167 might also result in a requirement to manually update the bundled rails-ujs code.

I'll set this issue to *private* given the possible implications.

Related issues:

Has duplicate Redmine - Feature #34062: Upgrade Rails to 5.2.4.5	**Closed**

Associated revisions

Revision 20789 - 2021-03-15 14:16 - Go MAEDA

Update Rails to 5.2.4.5 (#33906).

Patch by Marius BALTEANU.

Revision 20790 - 2021-03-15 14:17 - Go MAEDA

Update Rails UJS to 5.2.4.5 unminified (#33906).

Patch by Marius BALTEANU.

Revision 20791 - 2021-03-15 14:30 - Go MAEDA

Update JavaScript filename (#33906).

Patch by Marius BALTEANU.

Revision 20793 - 2021-03-15 15:15 - Go MAEDA

Merged r20789 from trunk to 4.1-stable (#33906).

Revision 20794 - 2021-03-15 15:22 - Go MAEDA

Update Rails UJS to 5.2.4.5 unminified for 4.1-stable (#33906).

Revision 20795 - 2021-03-15 15:31 - Go MAEDA

Update JavaScript filename for 4.1-stable (#33906).

Revision 20797 - 2021-03-15 15:39 - Go MAEDA

Merged r20789 from trunk to 4.0-stable (#33906).

Revision 20798 - 2021-03-15 16:16 - Go MAEDA

Backport #31205 to 4.0-stable in order to update Rails UJS (#33906).

Revision 20799 - 2021-03-15 16:25 - Go MAEDA

Update Rails UJS to 5.2.4.5 unminified for 4.0-stable (#33906).

Revision 20800 - 2021-03-15 16:34 - Go MAEDA

Update JavaScript filename for 4.0-stable (#33906).

History

#1 - 2020-08-26 16:23 - Go MAEDA

Thank you for reporting the issue. I had missed the release.

Mischa The Evil wrote:

> Note: the fix for CVE-2020-8167 might also result in a requirement to manually update the bundled rails-ujs code.

Do you know how to build a new public/javascripts/jquery-*-ui-*-ujs-*.js?

#2 - 2020-08-28 01:32 - Mischa The Evil

Go MAEDA wrote:

> Mischa The Evil wrote:
>
> > Note: the fix for CVE-2020-8167 might also result in a requirement to manually update the bundled rails-ujs code.
>
> Do you know how to build a new public/javascripts/jquery-*-ui-*-ujs-*.js?

I do not, though given the remaining[1] history, I think Marius should be able to tell this.

[1] the last update of the file in r19803 destroyed the file's prior history in SCM.

#3 - 2020-10-04 19:54 - Marius BĂLTEANU

- Target version set to 4.0.8

I manually maintain public/javascripts/jquery-*-ui-*-ujs-*.js? by replacing the old versions of the JS libraries with the new versions.

Regarding rails-ujs, the file is part of the actionview gem and the new version can be found in lib/assets/compiled/rails-ujs.js, but it's not minified and from what I remember, I used an online tool at that time. We can do the same now or we can add it non minified until we adopt a JS package tool to manage the dependencies.

Rails was updated by Jean-Philippe in #34062, I'm assigning this as well to update rails-ujs.

#4 - 2020-12-14 08:16 - Mischa The Evil

- Blocks Feature #34062: Upgrade Rails to 5.2.4.5 added

#5 - 2020-12-16 08:23 - Marius BĂLTEANU

- Assignee set to Jean-Philippe Lang

#6 - 2021-03-09 05:55 - Bernhard Rohloff

JPL committed the patch for updating Rails to 5.2.4.4 five month ago (r20109). As it's no longer a thing, shall we close this issue and perhaps #34062 , too?

#7 - 2021-03-09 06:09 - Bernhard Rohloff

Marius BALTEANU wrote:

> I manually maintain public/javascripts/jquery-*-ui-*-ujs-*.js? by replacing the old versions of the JS libraries with the new versions.
>
> Regarding rails-ujs, the file is part of the actionview gem and the new version can be found in lib/assets/compiled/rails-ujs.js, but it's not minified and from what I remember, I used an online tool at that time. We can do the same now or we can add it non minified until we adopt a JS

> package tool to manage the dependencies.
>
> Rails was updated by Jean-Philippe in #34062, I'm assigning this as well to update rails-ujs.

Okay, didn't read that beforehand. Sorry. Reading before writing is always a good habit. *facepalm*

#8 - 2021-03-15 08:28 - Marius BĂLTEANU

- File 0001-Update-Rails-to-5.2.4.5.patch added

- File 0002-Update-Rails-UJS-to-5.2.4.5-unminified.patch added

- File 0003-Update-javascript-filename.patch added

- Assignee changed from Jean-Philippe Lang to Go MAEDA

Adding a patch that:

- Updates Rails to 5.2.4.5 which includes another security fix.
- Updates Rails UJS to 5.2.4.5 unminified in order to avoid this manual step.

All tests pass: https://gitlab.com/redmine-org/redmine/-/pipelines/270145466 (except some flaky system tests).

#9 - 2021-03-15 08:30 - Marius BĂLTEANU

- Subject changed from Update to Rails 5.2.4.3 to Update to Rails 5.2.4.5

#10 - 2021-03-15 14:30 - Go MAEDA

- Status changed from New to Resolved

- Resolution set to Fixed

Committed the patches. Thank you.

#11 - 2021-03-15 16:34 - Go MAEDA

- Status changed from Resolved to Closed

#12 - 2021-03-15 17:06 - Marius BĂLTEANU

- Blocks deleted (Feature #34062: Upgrade Rails to 5.2.4.5)

#13 - 2021-03-15 17:06 - Marius BĂLTEANU

- Private changed from Yes to No

#14 - 2021-03-15 17:06 - Marius BĂLTEANU

- Has duplicate Feature #34062: Upgrade Rails to 5.2.4.5 added

#15 - 2021-03-15 17:07 - Marius BĂLTEANU

- Tracker changed from Defect to Feature

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

Files

0001-Update-Rails-to-5.2.4.5.patch	642 Bytes	2021-03-15	Marius BĂLTEANU
0003-Update-javascript-filename.patch	1.34 KB	2021-03-15	Marius BĂLTEANU
0002-Update-Rails-UJS-to-5.2.4.5-unminified.patch	99.3 KB	2021-03-15	Marius BĂLTEANU