# Redmine - Defect #32563

## Redmine 4 crashing with SEGFAULT under stress test when Markdown is used

2019-12-08 14:20 - Martin Cizek

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | | **% Done:** | 0% |
| **Category:** | Text formatting | **Estimated time:** | 0.00 hour |
| **Target version:** | | | |
| **Resolution:** | Wont fix | **Affected version:** | 4.0.5 |

**Description**

Disclosure: my real motivation is to provide even more ammunition for #32424. But this issue is still valid and represents also a DOS and possibly other security vulnerability.

The Redcarpet-based wiki formatter is shared in Redmine, see source:trunk/lib/redmine/wiki_formatting/markdown/formatter.rb. I guess that with Rails 5 on Redmine 4, multithreaded operation became available by default. And when the app server supports multithreading, it just happens that Redmine is multithreaded (not a Rails expert). Redcarpet instance is not thread-safe - I've found this issue, opened for more than three years atm.

Steps to reproduce:

- docker run redmine4 Note[1]
- Configure markdown as rext formatting,  create some larger wiki pages, create an API key
- Run a stress test with parallel requests, we were using 12 workers invoking curl -sf -g -H "X-Redmine-API-Key: $api_key" -o "$o" "$url/$q"

[1] Yes, it's using not recommended Webrick within rails server, still hope it's not an excuse for this behavior. :) Actually, we first came across this when creating a rake task for processing markup format conversions in parallel. But it happened also when we were doing rendering tests using standard Redmine stack, which is this issue.

Expected result: everything is rendering fine.

Actual result: ruby segfaults after a few hundred pages rendered.

```
ruby: markdown.c:2896: sd_markdown_render: Assertion `md->work_bufs[BUFFER_SPAN].size == 0' failed
.
/usr/src/redmine/lib/redmine/wiki_formatting/markdown/formatter.rb:82: [BUG] Segmentation fault at
 0x0000000000000000
ruby 2.6.5p114 (2019-10-01 revision 67812) [x86_64-linux]
```

Possible solutions:

- Do not share Redcarpet formatter
- Mutex it
- Make it thread local
- Document that multithreaded operation must be prevented when Markdown is used
- Get rid of Redcarpet (yes, please! Plus #32424)

**Related issues:**

| | |
|---|---|
| Related to Redmine - Feature #32424: CommonMark Markdown Text Formatting | **Closed** |
| Has duplicate Redmine - Defect #40131: markdown/formatter.rb:81: [BUG] Segmen... | **Closed** |

### History

**#1 - 2019-12-08 14:23 - Go MAEDA**

*- Related to Feature #32424: CommonMark Markdown Text Formatting added*

**#2 - 2021-08-12 23:04 - Marius BĂLTEANU**

*- Status changed from New to Closed*

*- Resolution set to Wont fix*

The current Markdown implementation based on RedCarpet is going to be dropped in the future versions and it will be replaced by the CommonMark Markdown (Github Flavoured) formatter that was just committed for 5.0.0.

**#3 - 2024-01-26 15:24 - Holger Just**

*- Has duplicate Defect #40131: markdown/formatter.rb:81: [BUG] Segmentation fault at 0x0000000000000000 added*