

Redmine - Defect #29756

\f or \v character in Textile markup may cause RegexpError exception

2018-10-11 08:47 - Hide MATSUTANI

Status:	Closed	Start date:	
Priority:	Normal	Due date:	
Assignee:	Go MAEDA	% Done:	0%
Category:	Text formatting	Estimated time:	0.00 hour
Target version:	3.4.7	Affected version:	3.4.4
Resolution:	Fixed		

Description

When I make a new issue which includes some control codes, Redmine goes internal error but the issue is created. Then I go back to the previous view and refer the issue, Redmine goes internal error again.

I tested some cases and found that in the NG case, the text starts with 0x20 0x0B.
If it starts with only 0x0B, the problem doesn't occur.

- NG case

ADDRESS +0 +1 +2 +3 +4 +5 +6 +7 +8 +9 +A +B +C +D +E +F 0123456789ABCDEF

-----+-----

00000000: 20 0B 61 62 63 64 65 31 32 33 34 35 20 -- -- -- .abcde12345

- OK case

ADDRESS +0 +1 +2 +3 +4 +5 +6 +7 +8 +9 +A +B +C +D +E +F 0123456789ABCDEF

-----+-----

00000000: 0B 61 62 63 64 65 31 32 33 34 35 20 -- -- -- -- .abcde12345

Even if the text contains the control codes, redmine should not goes internal error, I think.

In order to reproduce the defect, please use the attached file.
Open it in the text editor and paste it in the description of the new issue in Redmine.

Related issues:	
Related to Redmine - Defect #32971: New line between list items break a list	Closed

Associated revisions

Revision 17603 - 2018-10-28 12:01 - Go MAEDA

\f or \v character in Textile markup may cause RegexpError exception (#29756).

Patch by Go MAEDA.

Revision 17604 - 2018-10-28 12:04 - Go MAEDA

Merged r17603 from trunk to 3.4-stable (#29756).

History

- #1 - 2018-10-11 14:12 - Go MAEDA
Could you provide your environment information that you can see on /admin/info page? It is even better if you provide errors in production.log.
- #2 - 2018-10-11 17:00 - Go MAEDA
Confirmed the problem. You can create an issue but you will see Internal Server Error when accessing issues#show page.

```
Processing by IssuesController#show as HTML
Parameters: {"id"=>"20368"}
Current user: admin (id=1)
```

```
Rendered issues/_action_menu.html.erb (4.8ms)
Rendered issues/show.html.erb within layouts/base (2326.0ms)
Completed 500 Internal Server Error in 2394ms (ActiveRecord: 52.4ms)
```

```
ActionView::Template::Error (too big number for repeat range: /^ {100001}\S/):
85:
86:   <p><strong><%=l(:field_description)%></strong></p>
87:   <div class="wiki">
88:     <%= textilizable @issue, :description, :attachments => @issue.attachments %>
89:   </div>
90: </div>
91: <% end %>
lib/redmine/wiki_formatting/textile/redcloth3.rb:1037:in `flush_left'
lib/redmine/wiki_formatting/textile/redcloth3.rb:1031:in `clean_white_space'
lib/redmine/wiki_formatting/textile/redcloth3.rb:293:in `to_html'
lib/redmine/wiki_formatting/textile/formatter.rb:43:in `to_html'
lib/redmine/wiki_formatting.rb:89:in `to_html'
app/helpers/application_helper.rb:656:in `textilizable'
app/views/issues/show.html.erb:88:in `_app_views_issues_show_html_erb__2452628678795344758_70339042017100'
app/controllers/issues_controller.rb:106:in `block (2 levels) in show'
app/controllers/issues_controller.rb:99:in `show'
lib/redmine/sudo_mode.rb:63:in `sudo_mode'
```

#3 - 2018-10-11 17:03 - Go MAEDA

The issue is reproducible when the text formatting setting is Textile. No problem if the setting is Markdown.

#4 - 2018-10-11 18:28 - Go MAEDA

Here is a workaround.

```
Index: lib/redmine/wiki_formatting/textile/redcloth3.rb
=====
--- lib/redmine/wiki_formatting/textile/redcloth3.rb      (revision 17592)
+++ lib/redmine/wiki_formatting/textile/redcloth3.rb      (working copy)
@@ -1034,7 +1034,7 @@
     def flush_left( text )
       indt = 0
       if text =~ /^ /
-         while text !~ /^ {#{indt}}\S/
+         while text !~ /^ {#{indt}}[^ ]/
           indt += 1
         end unless text.empty?
         if indt.nonzero?
```

If the string variable text start with "\x0b", the while loop never ends until some error occurs. It is the cause of the error. The regexp /^ {1}\S/ does not match the string "\x0b" because "\x0b" is considered as white-space. In other words, \S/ matches "\x0b" because "\x0b" is a kind of white-space.

Maybe the regular expression /^ {#{indt}}\S/ is expected to match preceeding space characters and a character other than space char, so it may be expected to match "\x0b" too. But \S does not match "\x0b". It matches not only space character but [^\t\r\n\f\v]. "\v" is another expression of "\x0b".

#5 - 2018-10-12 03:09 - Go MAEDA

Does anyone understand why the implementation of flush_left method is so complicated? I think we can make it simpler like the following:

```
Index: lib/redmine/wiki_formatting/textile/redcloth3.rb
=====
--- lib/redmine/wiki_formatting/textile/redcloth3.rb      (revision 17592)
+++ lib/redmine/wiki_formatting/textile/redcloth3.rb      (working copy)
@@ -1032,15 +1032,7 @@
     end

     def flush_left( text )
-      indt = 0
-      if text =~ /^ /
-         while text !~ /^ {#{indt}}\S/
-           indt += 1
-         end unless text.empty?
-         if indt.nonzero?
-           text.gsub!( /^ {#{indt}}/, ' ' )
-         end
-       end
+      text.sub!( / ^ +/, ' ' )
     end
```

```
def footnote_ref( text )
```

#6 - 2018-10-12 03:45 - Hide MATSUTANI

Maeda-san

Thank you for the consideration.

That's exactly the same as my problem. The log looks same as mine.

I will try the suggested workaround. Thank you.

I put my environment info for future reference.

Environment:

Redmine version	3.4.4.stable.17236
Ruby version	2.4.3-p205 (2017-12-14) [x86_64-linux]
Rails version	4.2.8
Environment	production
Database adapter	Mysql2

SCM:

Subversion	1.7.14
Git	1.8.3.1
Filesystem	

Redmine plugins:

clipboard_image_paste	1.12
recurring_tasks	2.0.0-pre
redmine_banner	0.1.2
redmine_comment_only	0.0.1
redmine_enter_cancel	0.0.2
redmine_export_with_journals	0.0.8
redmine_issue_templates	0.1.8
redmine_knowledgebase	3.3.1
redmine_pivot_table	0.0.5
redmine_wiki_lists	0.0.9
redmine_wiki_unc	0.0.3
sidebar_hide	0.0.8
view_customize	1.1.4

#7 - 2018-10-12 03:50 - Hide MATSUTANI

Opps, the cases should be reversed in the description.

- NG case

ADDRESS	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F	0123456789ABCDEF
-----+-----																	
00000000:	0B	61	62	63	64	65	31	32	33	34	35	20	--	--	--	--	.abcde12345

- OK case

ADDRESS	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F	0123456789ABCDEF
-----+-----																	
00000000:	20	0B	61	62	63	64	65	31	32	33	34	35	20	--	--	--	.abcde12345

#8 - 2018-10-12 11:13 - Go MAEDA

- Target version set to Candidate for next minor release

#9 - 2018-10-14 04:32 - Go MAEDA

- File fix-29756.diff added

- Target version changed from Candidate for next minor release to 3.4.7

Here is a patch. Added a test to the code in [#29756#note-4](#).

#10 - 2018-10-14 04:47 - Go MAEDA

- Subject changed from Internal Error when new issue includes some control code to \f and \v characters in Textile markup may cause RegexpError exception

- Category changed from Issues to Text formatting

#11 - 2018-10-14 05:36 - Go MAEDA

Hide MATSUTANI wrote:

Opps, the cases should be reversed in the description.

No, cases in the description field are correct. 0x20 and 0x0b at the beginning of a line cause the exception.

#12 - 2018-10-14 15:20 - Hide MATSUTANI

Go MAEDA wrote:

Hide MATSUTANI wrote:

Opps, the cases should be reversed in the description.

No, cases in the description field are correct. 0x20 and 0x0b at the beginning of a line cause the exception.

Maeda-san

Sorry, I was confused.
Thank you for preparing patch.

#13 - 2018-10-15 17:31 - Go MAEDA

- File fix-29756-v2.diff added

#14 - 2018-10-28 12:02 - Go MAEDA

- Subject changed from `\f` and `\v` characters in Textile markup may cause `RegexpError` exception to `\f` or `\v` character in Textile markup may cause `RegexpError` exception
- Status changed from New to Resolved
- Assignee set to Go MAEDA
- Resolution set to Fixed

#15 - 2018-10-28 12:05 - Go MAEDA

- Status changed from Resolved to Closed

Committed.

#16 - 2020-02-18 13:18 - Go MAEDA

- Related to Defect #32971: New line between list items break a list added

Files			
NG_sample.txt	13 Bytes	2018-10-11	Hide MATSUTANI
OK_sample.txt	12 Bytes	2018-10-11	Hide MATSUTANI
fix-29756.diff	1.16 KB	2018-10-14	Go MAEDA
fix-29756-v2.diff	1.21 KB	2018-10-15	Go MAEDA