

Ruby - Bug #13526

Segmentation fault at 0x0055c2e58e8920 ruby 2.3.1p112 (2016-04-26 revision 54768) [x86_64-linux]

04/28/2017 07:31 PM - vlad-leonov (Vladislav Leonov)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 2.3.1p112 (2016-04-26 revision 54768) [x86_64-linux]	Backport: 2.2: UNKNOWN, 2.3: DONE, 2.4: DONE
Description see attached log		

Associated revisions

Revision c7ff36c6f083f59ea5f063e5501ceb19c049fe30 - 05/07/2017 04:26 AM - Eric Wong

variable.c: cleanup waitq upon thread death

- variable.c (autoload_reset): use idempotent list_del_init (autoload_sleep): moved code from rb_autoload_load (autoload_sleep_done): cleanup for use with rb_ensure (rb_autoload_load): ensure list delete happens in case the thread dies during sleep
- test/ruby/bug-13526.rb: new script for separate execution
- test/ruby/test_autoload.rb (test_bug_13526): new test [ruby-core:81016] [Bug #13526]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@58587 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision c7ff36c6 - 05/07/2017 04:26 AM - Eric Wong

variable.c: cleanup waitq upon thread death

- variable.c (autoload_reset): use idempotent list_del_init (autoload_sleep): moved code from rb_autoload_load (autoload_sleep_done): cleanup for use with rb_ensure (rb_autoload_load): ensure list delete happens in case the thread dies during sleep
- test/ruby/bug-13526.rb: new script for separate execution
- test/ruby/test_autoload.rb (test_bug_13526): new test [ruby-core:81016] [Bug #13526]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@58587 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision b5b1a213ec5cbde6adaf0d37953ff05c393218b - 05/09/2017 03:42 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 58587,58588: [Backport #13526]

```
variable.c: cleanup waitq upon thread death
```

```
* variable.c (autoload_reset): use idempotent list_del_init
(autoload_sleep): moved code from rb_autoload_load
(autoload_sleep_done): cleanup for use with rb_ensure
(rb_autoload_load): ensure list delete happens in case the
thread dies during sleep
* test/ruby/bug-13526.rb: new script for separate execution
* test/ruby/test_autoload.rb (test_bug_13526): new test
[ruby-core:81016] [Bug #13526]
* properties.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_4@58637 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision b5b1a213 - 05/09/2017 03:42 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 58587,58588: [Backport #13526]

```
variable.c: cleanup waitq upon thread death
```

```
* variable.c (autoload_reset): use idempotent list_del_init
(autoload_sleep): moved code from rb_autoload_load
(autoload_sleep_done): cleanup for use with rb_ensure
(rb_autoload_load): ensure list delete happens in case the
thread dies during sleep
* test/ruby/bug-13526.rb: new script for separate execution
* test/ruby/test_autoload.rb (test_bug_13526): new test
[ruby-core:81016] [Bug #13526]
* properties.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_4@58637 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 8f01d618e8e4960265696f0ea11cbcb941fc2ce - 06/30/2017 10:52 AM - U.Nakamura

merge revision(s) 58587,58588: [Backport #13526]

```
variable.c: cleanup waitq upon thread death
```

```
* variable.c (autoload_reset): use idempotent list_del_init
(autoload_sleep): moved code from rb_autoload_load
(autoload_sleep_done): cleanup for use with rb_ensure
(rb_autoload_load): ensure list delete happens in case the
thread dies during sleep
* test/ruby/bug-13526.rb: new script for separate execution
* test/ruby/test_autoload.rb (test_bug_13526): new test
[ruby-core:81016] [Bug #13526]
* properties.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@59219 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 8f01d618 - 06/30/2017 10:52 AM - U.Nakamura

merge revision(s) 58587,58588: [Backport #13526]

```
variable.c: cleanup waitq upon thread death
```

```
* variable.c (autoload_reset): use idempotent list_del_init
(autoload_sleep): moved code from rb_autoload_load
(autoload_sleep_done): cleanup for use with rb_ensure
(rb_autoload_load): ensure list delete happens in case the
thread dies during sleep
* test/ruby/bug-13526.rb: new script for separate execution
* test/ruby/test_autoload.rb (test_bug_13526): new test
[ruby-core:81016] [Bug #13526]
* properties.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@59219 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 05/01/2017 01:22 PM - wanabe (_ wanabe)

vlad-leonov (Vladislav Leonov) wrote:

```
-- Ruby level backtrace information -----
/home/vlad/.rbenv/versions/2.3.1/lib/ruby/gems/2.3.0/gems/puma-3.8.2/lib/puma/thread_pool.rb:120:in block in spawn_thread'
```

Ruby level backtrace shows there are some threads.

```
-- C level backtrace information -----
/home/vlad/.rbenv/versions/2.3.1/bin/ruby(rb_vm_bugreport+0x535) [0x55c2e5985175] vm_dump.c:688
/home/vlad/.rbenv/versions/2.3.1/bin/ruby(rb_bug_context+0xd1) [0x55c2e5961f71] error.c:435
/home/vlad/.rbenv/versions/2.3.1/bin/ruby(sigsegv+0x3e) [0x55c2e585c3ee] signal.c:890
/lib/x86_64-linux-gnu/libpthread.so.0 [0x7fb325847390]
/home/vlad/.rbenv/versions/2.3.1/bin/ruby(autoload_reset+0xa3) [0x55c2e58acd43] variable.c:2129
/home/vlad/.rbenv/versions/2.3.1/bin/ruby(rb_ensure+0xf0) [0x55c2e57991f0] eval.c:906
/home/vlad/.rbenv/versions/2.3.1/bin/ruby(rb_autoload_load+0x156) [0x55c2e58b3156] variable.c:2190
/home/vlad/.rbenv/versions/2.3.1/bin/ruby(rb_const_get_0.constprop.24+0x104) [0x55c2e58b3304] variable.c:2243
```

C level backtrace suggests that the issue may be related to autoload.

I found same issue on rails/rails repository. <https://github.com/rails/rails/issues/27455>

Here is a reduced script.

This code causes SEGV with a 60-70% possibility as far as I see.

```
sleep if $load
$load = true

n = 10
threads = Array.new(n) do
  Thread.new do
    begin
      autoload :Foo, "#{File.dirname($0)}/#{ $0}"
      Thread.pass
      Foo
    ensure
      Thread.pass
    end
  end
end

Thread.pass while threads.all?(&:stop?)
100.times { Thread.pass }
```

#2 - 05/01/2017 01:31 PM - usa (Usaku NAKAMURA)

- File *segv.log* added

- Description updated

- Backport changed from 2.2: UNKNOWN, 2.3: UNKNOWN, 2.4: UNKNOWN to 2.2: UNKNOWN, 2.3: REQUIRED, 2.4: UNKNOWN

#3 - 05/01/2017 01:33 PM - usa (Usaku NAKAMURA)

It seems that the HEAD of ruby_2_3 still has this problem but trunk nor ruby_2_4 don't.

#4 - 05/01/2017 02:01 PM - wanabe (_ wanabe)

- File *bug13526.log* added

I'm sorry to reproduce with trunk at my environment.
Log attached.

#5 - 05/01/2017 08:29 PM - usa (Usaku NAKAMURA)

- Backport changed from 2.2: UNKNOWN, 2.3: REQUIRED, 2.4: UNKNOWN to 2.2: UNKNOWN, 2.3: REQUIRED, 2.4: REQUIRED

wanabe (_ wanabe) wrote:

I'm sorry to reproduce with trunk at my environment.

Oh, thank you.

#6 - 05/07/2017 02:44 AM - wanabe (_ wanabe)

- File *bug13526_dp.log* added

- File *bug13526_dp.patch* added

git bisect shows that this issue is appeared at r52332 [Bug [#11384](#)].

I ran <https://bugs.ruby-lang.org/issues/13526#note-1> script with attached debug-print patch and got the log.

1. Thread 0x000055eacc7089d0 had "waitq: 0x7f737581fa18" on the stack. (line 4)
2. Thread 0x000055eacc7089d0 was killed and its stack was shrunked. (line 20)
3. rb_autoload_reset() tried to delete "waitq: 0x7f737581fa18" from list. (line 22)
4. But the node have been out of stack and corrupted!

And the log alerts us that check_autoload_required() returns inconsistent values.

I guess this is caused by the flow: rb_autoload_str() -> rb_const_set(mod, id, Qundef) -> const_tbl_update() -> autoload_delete() -> st_delete(RCLASS_IV_TBL(mod), &autoload, &val).
(But maybe other issue...)

#7 - 05/07/2017 03:51 AM - normalperson (Eric Wong)

s.wanabe@gmail.com wrote:

git bisect shows that this issue is appeared at r52332 [Bug [#11384](#)].

I ran <https://bugs.ruby-lang.org/issues/13526#note-1> script with attached debug-print patch and got the log.

Thank you! Fix coming.

#8 - 05/07/2017 04:26 AM - Anonymous

- Status changed from Open to Closed

Applied in changeset trunk|r58587.

variable.c: cleanup waitq upon thread death

- variable.c (autoload_reset): use idempotent list_del_init (autoload_sleep): moved code from rb_autoload_load (autoload_sleep_done): cleanup for use with rb_ensure (rb_autoload_load): ensure list delete happens in case the thread dies during sleep
- test/ruby/bug-13526.rb: new script for separate execution
- test/ruby/test_autoload.rb (test_bug_13526): new test [[ruby-core:81016](#)] [Bug [#13526](#)]

#9 - 05/07/2017 04:31 AM - normalperson (Eric Wong)

Eric Wong normalperson@yhbt.net wrote:

s.wanabe@gmail.com wrote:

git bisect shows that this issue is appeared at r52332 [Bug [#11384](#)].

I ran <https://bugs.ruby-lang.org/issues/13526#note-1> script with attached debug-print patch and got the log.

Thank you! Fix coming.

OK, committed as r58587 with that script.

Everyone: In the future, feel free to Cc: me regarding any problems I may have (even tangentially) caused. I am on many mailing lists so I prioritize stuff I'm Cc-ed on. Thanks.

#10 - 05/07/2017 05:41 AM - wanabe (_ wanabe)

normalperson (Eric Wong) wrote:

OK, committed as r58587 with that script.

Thank you!

It works perfectly as far as I can see.

Everyone: In the future, feel free to Cc: me regarding any problems I may have (even tangentially) caused. I am on many mailing lists so I prioritize stuff I'm Cc-ed on. Thanks.

Sorry. I've commented by Redmine with my web browser, so I could not Cc: you. So I add you as the watcher. Does Redmine Cc this comment to you?

#11 - 05/07/2017 06:02 AM - normalperson (Eric Wong)

s.wanabe@gmail.com wrote:

normalperson (Eric Wong) wrote:

OK, committed as r58587 with that script.

Thank you!

It works perfectly as far as I can see.

Thank you for confirming. Your small reproduction script was very helpful.

Everyone: In the future, feel free to Cc: me regarding any problems I may have (even tangentially) caused. I am on many mailing lists so I prioritize stuff I'm Cc-ed on. Thanks.

Sorry. I've commented by Redmine with my web browser, so I could not Cc: you.
So I add you as the watcher. Does Redmine Cc this comment to you?

Yes, adding as redmine watcher works for me. Thanks.

#12 - 05/09/2017 03:42 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.2: UNKNOWN, 2.3: REQUIRED, 2.4: REQUIRED to 2.2: UNKNOWN, 2.3: REQUIRED, 2.4: DONE

ruby_2_4 r58637 merged revision(s) 58587,58588.

#13 - 06/30/2017 10:52 AM - usa (Usaku NAKAMURA)

- Backport changed from 2.2: UNKNOWN, 2.3: REQUIRED, 2.4: DONE to 2.2: UNKNOWN, 2.3: DONE, 2.4: DONE

ruby_2_3 r59219 merged revision(s) 58587,58588.

#14 - 11/19/2017 03:22 PM - Eregon (Benoit Daloze)

Note that the original example only works if it's a file under the current directory invoked like "ruby test.rb",
Otherwise "#{File.dirname(\$0)}/#{ \$0}" does not refer to the current file.
I fixed it in r60854, to use File.expand_path(__FILE__).

The bug still happens on 2.4.1 whether the file exists or not, so it seems fine to test the case where the file does exist.
The bug seems caused by the interaction of autoload threads and the shutdown triggered by the main thread.

Files			
segv.log	245 KB	05/01/2017	usa (Usaku NAKAMURA)
bug13526.log	13.7 KB	05/01/2017	wanabe (_ wanabe)
bug13526_dp.patch	2.72 KB	05/07/2017	wanabe (_ wanabe)
bug13526_dp.log	12.5 KB	05/07/2017	wanabe (_ wanabe)