

Ruby - Bug #13605

GC bug calling `ObjectSpace.each\_object`

05/27/2017 08:09 PM - ryanf (Ryan Fitzgerald)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.4.1p111 (2017-03-22 revision 58053) [x86_64-linux]	Backport:	2.2: DONTNEED, 2.3: DONTNEED, 2.4: DONE
Description This code made Ruby bail out with the message "[BUG] rb_gc_mark(): 0x000000040dc740 is T_NONE": <pre>ObjectSpace.each_object(Module){ m next if (to_ignore.include?(m) rescue true) if m.respond_to?(:instance_methods) candidates.concat m.instance_methods(false).collect(&:to_s) end }</pre> I haven't been able to repro, but it happened building Pry on Travis CI: https://travis-ci.org/ryandickson/ryandickson/jobs/236720971 The relevant logs are attached.			
Related issues:			
Related to Ruby - Bug #13155: Segfault testing Pry		Closed	
Related to Ruby - Bug #13537: ruby crash in rb_gc_mark		Closed	

Associated revisions

Revision fccbc2d278226a2dfe5cffe4918724b0110c5781 - 06/12/2017 02:20 AM - ko1 (Koichi Sasada)

- proc.c (get_local_variable_ptr): return found env ptr. Returned env will be used by write barrier at `bind_local_variable_set()'. [Bug #13605]
- test/ruby/test_proc.rb: add a test for this issue.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@59063 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision fccbc2d2 - 06/12/2017 02:20 AM - ko1 (Koichi Sasada)

- proc.c (get_local_variable_ptr): return found env ptr. Returned env will be used by write barrier at `bind_local_variable_set()'. [Bug #13605]
- test/ruby/test_proc.rb: add a test for this issue.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@59063 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 8343847b6ba6f1baf58b8a86429a747d5c5fdec8 - 08/04/2017 03:06 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 59063: [Backport #13605]

```
* proc.c (get_local_variable_ptr): return found env ptr. Returned env
  will be used by write barrier at `bind_local_variable_set()'.
  [Bug #13605]
```

```
* test/ruby/test_proc.rb: add a test for this issue.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_4@59503 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 8343847b - 08/04/2017 03:06 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 59063: [Backport #13605]

```
* proc.c (get_local_variable_ptr): return found env ptr. Returned env
will be used by write barrier at `bind_local_variable_set()'.
[Bug #13605]
```

```
* test/ruby/test_proc.rb: add a test for this issue.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_4@59503 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 05/29/2017 02:02 AM - shyouhei (Shyouhei Urabe)

What is to_ignore and candidates in your script? Is it possible for you to show us a step to reproduce your situation?

#2 - 05/30/2017 01:05 AM - wanabe (_ wanabe)

- File patch-for-2508d68e.patch added

- File Dockerfile added

I guess the code snippet is from pry. https://github.com/pry/pry/blob/c18601d6a4ff97d1b6599ccd9ffc8c63b8d8fccb/lib/pry/input_completer.rb#L172

Here are Dockerfile and patch for pry to reproduce the issue.

33 / 100 are aborted on my environment.

#3 - 06/03/2017 01:35 PM - robertgleeson (Robert Gleeson)

wanabe (_ wanabe) wrote:

I guess the code snippet is from pry.

https://github.com/pry/pry/blob/c18601d6a4ff97d1b6599ccd9ffc8c63b8d8fccb/lib/pry/input_completer.rb#L172

Here are Dockerfile and patch for pry to reproduce the issue.

33 / 100 are aborted on my environment.

Thanks wanabe.

shyouhei (Shyouhei Urabe) wrote:

What is to_ignore and candidates in your script? Is it possible for you to show us a step to reproduce your situation?

Hey Shyouhei,

The segfault happens while running the pry test suite, I guess you can try:

git clone <https://github.com/pry/pry.git>

cd pry

git checkout -t origin/respond_to-2.4-warnings

bundle

bundle exec rake

On Linux/Travis it happens all the time, on OSX it happens randomly but this script always reproduces the issue for me, usually on 3rd or 4th attempt:

```
begin
```

```
system "bundle exec rake"
```

```
end while $? .exitstatus == 0
```

I tried a workaround, by moving .collect(&:to_s) underneath candidates.sort!(...) but the bug just happens somewhere else then:

/Users/robert/pry/lib/pry/slop/option.rb:92: [BUG] rb_gc_mark(): 0x007f85ab35dc10 is T_NONE

ruby 2.4.1p111

c:0053 p:---- s:0277 e:000276 CFUNC :to_s

c:0052 p:0016 s:0273 e:000272 METHOD /Users/r/pry/lib/pry/slop/option.rb:92

A very similar segfault happens on ruby-head, here's the build log:

<https://travis-ci.org/pry/pry/jobs/239070625>

So I think it's an issue since 2.4 and on ruby HEAD as well.

#4 - 06/04/2017 12:11 AM - robertgleeson (Robert Gleeson)

Another case:

```
Ruby v2.4.1 (ruby), Pry v0.10.4, method_source v0.8.2, CodeRay v1.1.1, Pry::Slop v3.4.0
/home/travis/build/ry/ry/spec/ry_output_spec.rb:119: warning: assigned but unused variable - custom_io
...../ho
me/travis/build/ry/ry/lib/ry/ry_instance.rb:159: [BUG] rb_gc_mark(): 0x00000003556f88 is T_NONE
ruby 2.4.1p111 (2017-03-22 revision 58053) [x86_64-linux]
```

See: <https://travis-ci.org/ry/ry/jobs/239070622>

I don't think segv is directly related to Pry::InputCompleter, just luck that it sometimes happens there, sometimes from lib/ry/slop, and sometimes in ry_instance.rb, something seems wrong in the runtime.

#5 - 06/04/2017 10:46 PM - robertgleeson (Robert Gleeson)

The segfault no longer happens, since <https://github.com/ry/ry/pull/1611/commits/94316852f5c1114f3073876558085835f2cf5377>. if you want to reproduce a commit before that one should work, on the respond_to-2.4-warnings branch.

#6 - 06/04/2017 10:51 PM - robertgleeson (Robert Gleeson)

robertgleeson (Robert Gleeson) wrote:

The segfault no longer happens, since <https://github.com/ry/ry/pull/1611/commits/94316852f5c1114f3073876558085835f2cf5377>. if you want to reproduce a commit before that one should work, on the respond_to-2.4-warnings branch.

Spoke too soon, i think we just got lucky, it still happens when i try running the suite many times.

#7 - 06/11/2017 04:23 PM - wanabe (_ wanabe)

It seems to be for lack of write-barrier. (as _ko1 suggested at https://twitter.com/_ko1/status/871892183464370176)

The following script causes similar [BUG] about 50% of the time.

```
10000.times do |i|
  v = rand(2000)
  name = "n#{v}"
  value = Object.new
  TOPLEVEL_BINDING.local_variable_set name, value
end
```

It is helpful with "-DRGENGC_CHECK_MODE=2" build flag.

I met following output:

```
verify_internal_consistency_reachable_i: WB miss (O->Y) 0x000055f470054578 [3LM ] T_IMEMO env -> 0x000055f470
1cc770 [0 ] T_OBJECT (Object)
verify_internal_consistency_reachable_i: WB miss (O->Y) 0x000055f470054758 [3LM ] T_IMEMO env -> 0x000055f470
206920 [0 ] T_OBJECT (Object)
(snip)
a.rb:3: [BUG] gc_verify_internal_consistency: found internal inconsistency.
ruby 2.5.0dev (2017-06-11 trunk 59060) [x86_64-linux]
(snip)
```

#8 - 06/12/2017 02:20 AM - ko1 (Koichi Sasada)

- Status changed from Open to Closed

Applied in changeset trunk|r59063.

-
- proc.c (get_local_variable_ptr): return found env ptr. Returned env will be used by write barrier at `bind_local_variable_set()'.
[Bug #13605]
 - test/ruby/test_proc.rb: add a test for this issue.

#9 - 06/28/2017 12:45 AM - wanabe (_ wanabe)

- Related to Bug #13155: Segfault testing Pry added

#10 - 06/28/2017 03:07 AM - wanabe (_ wanabe)

- Related to Bug #13537: ruby crash in rb_gc_mark added

#11 - 06/28/2017 03:13 AM - wanabe (_ wanabe)

git bisect shows that the issue is come from r55766 [Feature #12628].
This commit is in ruby_2_4, but not in ruby_2_3 / ruby_2_2.

To core team:
Would you please set "Backport" of the ticket to "2.2: DONTNEED, 2.3: DONTNEED, 2.4: REQUIRED"?

#12 - 06/28/2017 03:37 AM - duerst (Martin Dürst)

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

#13 - 08/04/2017 03:06 PM - nagachika (Tomoyuki Chikanaga)

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

ruby_2_4 r59503 merged revision(s) 59063.

Files

each_object_bug.txt	81.9 KB	05/27/2017	ryanf (Ryan Fitzgerald)
patch-for-2508d68e.patch	8.07 KB	05/30/2017	wanabe (_ wanabe)
Dockerfile	353 Bytes	05/30/2017	wanabe (_ wanabe)