

Ruby - Bug #14421

super_method segfaults when called on a re-bound Method

01/29/2018 05:25 PM - rusterholz (Andy Rusterholz)

Status:Closed Priority:Normal Assignee: Target version: ruby -v:ruby 2.5.0p0 (2017-12-25 revision 61468) [x86_64-darwin17]		Backport:2.3: REQUIRED, 2.4: DONE, 2.5: DONE	
Description The line of code below causes a segfault on 2.5.0. This appears to possibly be related to #11419, but is not the same. The segfault is not limited to the String class used in the example; it can be reproduced with any class with at least one instance_method. More generally, it can be reproduced any time super_method is called on a Method which was formed by (validly) calling bind on an UnboundMethod. \$ ruby -e 'String.instance_method(:length).bind(String.new).super_method' -e:1: [BUG] Segmentation fault at 0x0000000000000018 ruby 2.5.0p0 (2017-12-25 revision 61468) [x86_64-darwin17] -- Crash Report log information ----- See Crash Report log file under the one of following: * ~/Library/Logs/DiagnosticReports * /Library/Logs/DiagnosticReports for more details. Don't forget to include the above Crash Report log file in bug reports. -- Control frame information ----- c:0003 p:---- s:0010 e:000009 CFUNC :super_method c:0002 p:0028 s:0006 e:000005 EVAL -e:1 [FINISH] c:0001 p:0000 s:0003 E:001570 (none) [FINISH] -- Ruby level backtrace information ----- -e:1:in `<main>'</div><div>-e:1:in `super_method' -- Machine register context ----- rax: 0x0000000000000000 rbx: 0x00007fc51f43e1e0 rcx: 0x00000000108308730 rdx: 0x0000000000000000 rdi: 0x00007fc52106fd18 rsi: 0x00000000108308730 rbp: 0x00007ffef7b78f80 rsp: 0x00007ffef7b78f40 r8: 0x00007fc51f4623b8 r9: 0x00000000108543fa0 r10: 0x00007fc51f5070e8 r11: 0x0000000000000016 r12: 0x0000000000000000 r13: 0x00007fc51f541860 r14: 0x0000000000000000 r15: 0x00007fc52106fd18 rip: 0x0000000010819a2eb rfl: 0x00000000000010246 -- C level backtrace information ----- 0 libruby.2.5.dylib0x00000000108274d17rb_vm_bugreport + 135 1 libruby.2.5.dylib0x000000001080f9988rb_bug_context + 472 2 libruby.2.5.dylib0x000000001081e9161sigsegv + 81 3 libsystem_platform.dylib0x00007ffff7e2c0f5a__sigtramp + 26 4 libruby.2.5.dylib0x0000000010819a2ebmethod_super_method + 43 5 libruby.2.5.dylib0x000000001082681fbvm_call_cfunc + 283 6 libruby.2.5.dylib0x00000000108251954vm_exec_core + 12196 7 libruby.2.5.dylib0x00000000108262acevm_exec + 142 8 libruby.2.5.dylib0x00000000108103501ruby_exec_internal + 177 9 libruby.2.5.dylib0x000000001081033f8ruby_run_node + 56 10 ruby0x00000000108086f2fmain + 79 -- Other runtime information -----			

```
* Loaded script: -e

* Loaded features:

 0 enumerator.so
 1 thread.rb
 2 rational.so
 3 complex.so
 4 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/x86_64-darwin17/enc/encdb.bundle
 5 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/x86_64-darwin17/enc/trans/transdb.bu
ndle
 6 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/x86_64-darwin17/rbconfig.rb
 7 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems/compatibility.rb
 8 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems/defaults.rb
 9 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems/deprecate.rb
10 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems/errors.rb
11 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems/version.rb
12 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems/requirement.rb
13 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems/platform.rb
14 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems/basic_specification.rb
15 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems/stub_specification.rb
16 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems/util/list.rb
17 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/x86_64-darwin17/stringio.bundle
18 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems/specification.rb
19 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems/exceptions.rb
20 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems/dependency.rb
21 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems/core_ext/kernel_gem.rb
22 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/monitor.rb
23 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems/core_ext/kernel_require.rb
24 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems.rb
25 /Users/rusterholz/.rvm/rubies/ruby-2.5.0/lib/ruby/2.5.0/rubygems/path_support.rb
```

Expected Results: Given that `String.new.method(:length).super_method` correctly returns `nil`, I would expect `String.instance_method(:length).bind(String.new).super_method` to also return `nil`.

Related issues:

Related to Ruby - Bug #13973: `super_method` fails on some `UnboundMethods`

Closed

Associated revisions

Revision b10b51225e039ccddd0ae1e68b66f731bfd8e40c - 01/30/2018 07:35 PM - Eric Wong

proc: fix `super_method` segfault after bind

- proc.c: handle undefined `iclass`
[ruby-core:85231] [Bug #14421]

From: Eric Wong e@80x24.org

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@62115 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision b10b5122 - 01/30/2018 07:35 PM - Eric Wong

proc: fix `super_method` segfault after bind

- proc.c: handle undefined `iclass`
[ruby-core:85231] [Bug #14421]

From: Eric Wong e@80x24.org

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@62115 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision aa58701dee09d609b792d1414a092d9e662f37da - 02/21/2018 04:36 AM - naruse (Yui NARUSE)

merge revision(s) 62115: [Backport #14421]

```
proc: fix super_method segfault after bind
```

```
* proc.c: handle undefined iclass
[ruby-core:85231] [Bug #14421]
```

From: Eric Wong <e@80x24.org>

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_5@62507 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision aa58701d - 02/21/2018 04:36 AM - naruse (Yui NARUSE)

merge revision(s) 62115: [Backport #14421]

proc: fix super_method segfault after bind

* proc.c: handle undefined iclass
[ruby-core:85231] [Bug #14421]

From: Eric Wong <e@80x24.org>

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_5@62507 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision f634fc1f8af020d24f3517249e567316e35e196a - 03/20/2018 04:21 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 62115: [Backport #14421]

proc: fix super_method segfault after bind

* proc.c: handle undefined iclass
[ruby-core:85231] [Bug #14421]

From: Eric Wong <e@80x24.org>

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_4@62866 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision f634fc1f - 03/20/2018 04:21 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 62115: [Backport #14421]

proc: fix super_method segfault after bind

* proc.c: handle undefined iclass
[ruby-core:85231] [Bug #14421]

From: Eric Wong <e@80x24.org>

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_4@62866 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 01/29/2018 05:38 PM - rusterholz (Andy Rusterholz)

- Description updated

#2 - 01/29/2018 05:41 PM - rusterholz (Andy Rusterholz)

- Description updated

#3 - 01/29/2018 05:42 PM - rusterholz (Andy Rusterholz)

- Description updated

#4 - 01/29/2018 05:54 PM - rusterholz (Andy Rusterholz)

Note: the above failing code correctly returns nil on a coworker's machine running ruby 2.4.2p198 (2017-09-14 revision 59899) [x86_64-darwin17].

#5 - 01/30/2018 01:08 AM - normalperson (Eric Wong)

andy@rusterholz.org wrote:

Note: the above failing code correctly returns nil on a coworker's machine running ruby 2.4.2p198 (2017-09-14 revision 59899) [x86_64-darwin17].

Thanks for simple test case, I guess the following patch is correct:

(sorry, I don't use "bind" or "super_method" at all, so maybe there's other problems but "make exam" passes for me)

```
--- a/proc.c
+++ b/proc.c
@@ -2725,6 +2725,7 @@ method_super_method(VALUE method)
```

```
TypedData_Get_Struct(method, struct METHOD, &method_data_type, data);
iclass = data->iclass;
+   if (!iclass) return Qnil;
super_class = RCLASS_SUPER(RCLASS_ORIGIN(iclass));
mid = data->me->called_id;
if (!super_class) return Qnil;
```

Full patch + test:

<https://80x24.org/spew/20180130004626.17796-1-e@80x24.org/raw>

#6 - 01/30/2018 07:35 PM - Anonymous

- Status changed from Open to Closed

Applied in changeset trunk|r62115.

proc: fix super_method segfault after bind

- proc.c: handle undefined iclass
[\[ruby-core:85231\]](#) [Bug [#14421](#)]

From: Eric Wong e@80x24.org

#7 - 01/31/2018 01:29 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: UNKNOWN to 2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: REQUIRED

#8 - 01/31/2018 01:32 AM - nagachika (Tomoyuki Chikanaga)

- Related to Bug [#13973](#): super_method fails on some UnboundMethods added

#9 - 01/31/2018 01:43 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: REQUIRED to 2.3: REQUIRED, 2.4: REQUIRED, 2.5: REQUIRED

I have confirmed the segfaults was reproducible with trunk/2.5.0, but wasn't with 2.4.3.

But this fault was introduced at r60127 ([#13973](#)), and I think r60127 should be backported.

r62115 should be backported with r60127.

I will fill REQUIRED for 2.3/2.4 in Backport field for this reason.

#10 - 02/21/2018 04:36 AM - naruse (Yui NARUSE)

- Backport changed from 2.3: REQUIRED, 2.4: REQUIRED, 2.5: REQUIRED to 2.3: REQUIRED, 2.4: REQUIRED, 2.5: DONE

ruby_2_5 r62507 merged revision(s) 62115.

#11 - 03/20/2018 04:21 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.3: REQUIRED, 2.4: REQUIRED, 2.5: DONE to 2.3: REQUIRED, 2.4: DONE, 2.5: DONE

ruby_2_4 r62866 merged revision(s) 62115.

Files

ruby_2018-01-29-102259_arusterholz-mbp15-9.crash	35.9 KB	01/29/2018	rusterholz (Andy Rusterholz)
--	---------	------------	------------------------------