Ruby trunk - Bug #13586

Ruby hangs when accessing array which is modified in instance_eval after Coverage.start

05/20/2017 04:36 PM - mtsmfm (Fumiaki Matsushima)

Status:	Assigned		
Priority:	Normal		
Assignee:	nobu (Nobuyoshi Nakada)		
Target version:			
ruby -v:	2.4.1	**Backport:**	2.2: UNKNOWN, 2.3: UNKNOWN, 2.4: UNKNOWN

Description

The following code will hang ruby:

```
# main.rb

require "coverage"

Coverage.start

require_relative "./foo"

# Perhaps we need more repetition to reproduce
1000.times do
  Foo.new.count
end

# foo.rb
class Foo
  attr_reader :foo

  def initialize
    @foo = []
    str = "add\n" * 1000 # Perhaps we need more repetition to reproduce
    instance_eval str, __FILE__, __LINE__
  end

  def count
    foo.count
  end

  def add
    @foo << nil
  end
end

$ docker run --rm -v $PWD:/app -w /app ruby:2.4.1 ruby main.rb
/app/foo.rb:7: [BUG] Segmentation fault at 0x00000000000001
ruby 2.4.1p111 (2017-03-22 revision 58053) [x86_64-linux]

-- Control frame information -----------------------------------------------
c:0007 p:---- s:0029 e:000028 CFUNC  :instance_eval
c:0006 p:0038 s:0022 e:000021 METHOD /app/foo.rb:7 [FINISH]
c:0005 p:---- s:0017 e:000016 CFUNC  :new
c:0004 p:0014 s:0013 e:000012 BLOCK  main.rb:9 [FINISH]
c:0003 p:---- s:0010 e:000009 CFUNC  :times
c:0002 p:0039 s:0006 e:000005 EVAL   main.rb:8 [FINISH]
c:0001 p:0000 s:0003 E:001930 (none) [FINISH]

-- Ruby level backtrace information ----------------------------------------
main.rb:8:in `<main>'
main.rb:8:in `times'
main.rb:9:in `block in <main>'
```

```
main.rb:9:in `new'
/app/foo.rb:7:in `initialize'
/app/foo.rb:7:in `instance_eval'

-- Machine register context ------------------------------------------------
 RIP: 0x00007f4230153599 RBP: 0x0000000000000001 RSP: 0x00007ffe62d245d0
 RAX: 0x0000000000000001 RBX: 0x00000000021e33c0 RCX: 0x0000000000000023
 RDX: 0x0000000000000000 RDI: 0x0000000000000001 RSI: 0x0000000000000000
  R8: 0x000000000000002a  R9: 0x0000000000000000 R10: 0x0000000000000000
 R11: 0x0000000000000000 R12: 0x0000000000000000 R13: 0x00000000021e3460
 R14: 0x0000000000000000 R15: 0x00000000022629f0 EFL: 0x0000000000010202

-- C level backtrace information -------------------------------------------
/usr/local/lib/libruby.so.2.4(rb_vm_bugreport+0x4f3) [0x7f4230306683] vm_dump.c:684
/usr/local/lib/libruby.so.2.4(rb_bug_context+0xd4) [0x7f42301853a4] error.c:506
/usr/local/lib/libruby.so.2.4(sigsegv+0x3e) [0x7f423027a05e] signal.c:907
/lib/x86_64-linux-gnu/libpthread.so.0 [0x7f422fed1890]
/usr/local/lib/libruby.so.2.4(iseq_setup+0xc9) [0x7f4230153599] compile.c:2476
/usr/local/lib/libruby.so.2.4(rb_iseq_compile_node+0x147) [0x7f4230154fe7] compile.c:673
/usr/local/lib/libruby.so.2.4(rb_iseq_new_with_opt+0x94) [0x7f42301cc184] iseq.c:483
/usr/local/lib/libruby.so.2.4(rb_iseq_compile_with_option+0x200) [0x7f42301cd250] iseq.c:650
/usr/local/lib/libruby.so.2.4(eval_string_with_cref+0x10c) [0x7f42302fb48c] vm_eval.c:1345
/usr/local/lib/libruby.so.2.4(rb_obj_instance_eval+0x16e) [0x7f42302fbb2e] vm_eval.c:1645
/usr/local/lib/libruby.so.2.4(vm_call_cfunc+0xef) [0x7f42302e8f3f] vm_insnhelper.c:1752
/usr/local/lib/libruby.so.2.4(vm_call_method+0xe3) [0x7f42302fab13] vm_insnhelper.c:2292
/usr/local/lib/libruby.so.2.4(vm_exec_core+0x1610) [0x7f42302f23d0] insns.def:1066
/usr/local/lib/libruby.so.2.4(vm_exec+0x8b) [0x7f42302f742b] vm.c:1727
/usr/local/lib/libruby.so.2.4(rb_call0+0x1ad) [0x7f42302fd4fd] vm_eval.c:62
/usr/local/lib/libruby.so.2.4(rb_class_new_instance+0x21) [0x7f42301f77f1] object.c:1896
/usr/local/lib/libruby.so.2.4(vm_call_cfunc+0xef) [0x7f42302e8f3f] vm_insnhelper.c:1752
/usr/local/lib/libruby.so.2.4(vm_call_method+0xe3) [0x7f42302fab13] vm_insnhelper.c:2292
/usr/local/lib/libruby.so.2.4(vm_exec_core+0x1610) [0x7f42302f23d0] insns.def:1066
/usr/local/lib/libruby.so.2.4(vm_exec+0x8b) [0x7f42302f742b] vm.c:1727
/usr/local/lib/libruby.so.2.4(invoke_iseq_block_from_c+0x516) [0x7f42302f8206] vm.c:969
/usr/local/lib/libruby.so.2.4(rb_yield_1+0xb4) [0x7f42302f8ea4] vm.c:1032
/usr/local/lib/libruby.so.2.4(int_dotimes+0x3e) [0x7f42301e6aee] numeric.c:4977
/usr/local/lib/libruby.so.2.4(vm_call_cfunc+0xef) [0x7f42302e8f3f] vm_insnhelper.c:1752
/usr/local/lib/libruby.so.2.4(vm_call_method+0xe3) [0x7f42302fab13] vm_insnhelper.c:2292
/usr/local/lib/libruby.so.2.4(vm_exec_core+0x113f) [0x7f42302f1eff] insns.def:967
/usr/local/lib/libruby.so.2.4(vm_exec+0x8b) [0x7f42302f742b] vm.c:1727
/usr/local/lib/libruby.so.2.4(ruby_exec_internal+0xb2) [0x7f423018b132] eval.c:244
/usr/local/lib/libruby.so.2.4(ruby_exec_node+0x1d) [0x7f423018cead] eval.c:308
/usr/local/lib/libruby.so.2.4(ruby_run_node+0x1e) [0x7f423018fa6e] eval.c:300
/usr/local/bin/ruby(main+0x4b) [0x40087b] main.c:36
```

I confirmed that this problem occurs on Ruby 2.4.0 and 2.4.1.
And I can't reproduce on Ruby 2.2.7 and 2.3.4

Full trace and code is https://gist.github.com/mtsmfm/b8c57c198793b7e7b835ae3255f0037c

History

#1 - 07/15/2017 03:08 AM - shyouhei (Shyouhei Urabe)

- Assignee set to nobu (Nobuyoshi Nakada)

- Status changed from Open to Assigned

#2 - 11/17/2017 08:20 PM - crazymykl (Mike MacDonald)

This also happens on 2.4.2p198, but not 2.5.0-preview1.