

Ruby - Bug #19994

Seemingly require causes segfault??

11/08/2023 09:55 AM - mtasaka (Mamoru TASAKA)

|                 |                                                             |                                                    |
|-----------------|-------------------------------------------------------------|----------------------------------------------------|
| Status:         | Closed                                                      |                                                    |
| Priority:       | Normal                                                      |                                                    |
| Assignee:       |                                                             |                                                    |
| Target version: |                                                             |                                                    |
| ruby -v:        | ruby 3.3.0dev (2023-11-08 master c8d4b103a9) [x86_64-linux] | Backport: 3.0: UNKNOWN, 3.1: UNKNOWN, 3.2: UNKNOWN |

**Description**

With [c8d4b103a9](#) , trying to execute stringex-2.8.6 <https://github.com/rsr/stringex/releases/tag/v2.8.6> testsuite seems to cause ruby segfault.

Trying to minimize code, the following causes segfault for almost all time (about 90%):

```
require 'test/unit'
require 'active_record'
```

ActiveRecord::Base.establish\_connection adapter: "sqlite3", database: ":memory:"

(strangely, with commenting out the first line i.e. require 'test/unit' segfault no longer occurs...)

**Backtrace:**

Thread 1 "ruby-mri" received signal SIGSEGV, Segmentation fault.

vm\_call\_cfunc\_with\_frame\_ (ec=0x55555555d1c0, reg\_cfp=0x7ffff7670b78, calling=<optimized out>, arg c=<optimized out>, argv=<optimized out>, stack\_bottom=<optimized out>)

at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86\_64/vm\_insnhelper.c:34

99

3499 int len = cfunc->argc;

Missing separate debuginfos, use: dnf debuginfo-install glibc-2.38.9000-17.fc40.x86\_64 gmp-6.2.1-5.fc39.x86\_64 libgcc-13.2.1-4.fc40.x86\_64 libxcrypt-4.4.36-2.fc39.x86\_64 libyaml-0.2.5-12.fc39.x86\_64 openssl-libs-3.1.4-1.fc40.x86\_64 rubygem-json-2.6.3-204.fc40.140.x86\_64 rubygem-sqlite3-1.6.1-2.fc40.140.x86\_64 sqlite-libs-3.44.0-1.fc40.x86\_64 zlib-1.2.13-5.fc40.x86\_64

(gdb) bt

#0 vm\_call\_cfunc\_with\_frame\_ (ec=0x55555555d1c0, reg\_cfp=0x7ffff7670b78, calling=<optimized out>, argc=<optimized out>, argv=<optimized out>, stack\_bottom=<optimized out>)

at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86\_64/vm\_insnhelper.c:34

99

#1 0x00007ffff7c5b62c in vm\_sendish (method\_explorer=<optimized out>, block\_handler=<optimized out>, cd=<optimized out>, reg\_cfp=<optimized out>, ec=<optimized out>)

at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86\_64/vm\_insnhelper.c:55

81

#2 vm\_exec\_core (ec=0x55555555d1c0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86\_64/redhat-linux-build/insns.def:822

#3 0x00007ffff7c739dd in rb\_vm\_exec (ec=0x55555555d1c0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86\_64/vm.c:2472

#4 0x00007ffff7c61463 in vm\_yield\_with\_cref (is\_lambda=0, cref=0x0, kw\_splat=0, argv=0x0, argc=0, ec=<optimized out>) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86\_64/vm.c:1622

#5 vm\_yield (kw\_splat=0, argv=0x0, argc=0, ec=<optimized out>) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86\_64/vm.c:1630

#6 rb\_yield\_0 (argv=0x0, argc=0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86\_64/vm\_eval.c:1362

#7 rb\_yield\_values2 (argc=0, argv=0x0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86\_64/vm\_eval.c:1408

#8 0x00007ffff7ad3b4f in rb\_ensure (b\_proc=0x7ffffde0fb990 <monitor\_sync\_body>, data1=140736888155080, e\_proc=0x7ffffde0fb6e0 <monitor\_sync\_ensure>, data2=<optimized out>)

at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86\_64/eval.c:1009

#9 0x00007ffff7c540c7 in vm\_call\_cfunc\_with\_frame\_ (ec=0x55555555d1c0, reg\_cfp=0x7ffff7670c20, calling=<optimized out>, argc=<optimized out>, argv=<optimized out>, stack\_bottom=<optimized out>)

at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86\_64/vm\_insnhelper.c:35

```

03
#10 0x00007ffff7c56641 in vm_sendish (ec=0x55555555d1c0, reg_cfp=0x7ffff7670c20, cd=<optimized out>, block_handler=<optimized out>, method_explorer=<optimized out>)
    at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm_callinfo.h:407
#11 0x00007ffff7c5d43f in vm_exec_core (ec=0x55555555d1c0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/redhat-linux-build/insns.def:802
#12 0x00007ffff7c739dd in rb_vm_exec (ec=0x55555555d1c0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm.c:2472
#13 0x00007ffff7b358fb in require_internal (ec=ec@entry=0x55555555d1c0, fname=<optimized out>, fname@entry=140736887218320, exception=exception@entry=1, warn=false)
    at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/load.c:1247
#14 0x00007ffff7b35e4e in rb_require_string_internal (fname=140736887218320) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/load.c:1346
#15 0x00007ffff7b35f08 in rb_require_string (fname=<optimized out>) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/load.c:1339
#16 0x00007ffff7c540c7 in vm_call_cfunc_with_frame_ (ec=0x55555555d1c0, reg_cfp=0x7ffff7670cc8, calling=<optimized out>, argc=<optimized out>, argv=<optimized out>, stack_bottom=<optimized out>)
    at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm_insnhelper.c:35
03
#17 0x00007ffff7c57b1f in vm_call_alias (ec=0x55555555d1c0, cfp=0x7ffff7670cc8, calling=0x7ffffffffffce00) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm_insnhelper.c:3873
#18 0x00007ffff7c5b62c in vm_sendish (method_explorer=<optimized out>, block_handler=<optimized out>, cd=<optimized out>, reg_cfp=<optimized out>, ec=<optimized out>)
    at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm_insnhelper.c:55
81
#19 vm_exec_core (ec=0x55555555d1c0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/redhat-linux-build/insns.def:822
#20 0x00007ffff7c739dd in rb_vm_exec (ec=0x55555555d1c0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm.c:2472
#21 0x00007ffff7b358fb in require_internal (ec=ec@entry=0x55555555d1c0, fname=<optimized out>, fname@entry=140736885373720, exception=exception@entry=1, warn=false)
    at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/load.c:1247
#22 0x00007ffff7b35e4e in rb_require_string_internal (fname=140736885373720) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/load.c:1346
#23 0x00007ffff7b35f08 in rb_require_string (fname=<optimized out>) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/load.c:1339
#24 0x00007ffff7c540c7 in vm_call_cfunc_with_frame_ (ec=0x55555555d1c0, reg_cfp=0x7ffff7670d70, calling=<optimized out>, argc=<optimized out>, argv=<optimized out>, stack_bottom=<optimized out>)
    at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm_insnhelper.c:35
03
#25 0x00007ffff7c57b1f in vm_call_alias (ec=0x55555555d1c0, cfp=0x7ffff7670d70, calling=0x7ffffffffffd3f0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm_insnhelper.c:3873
#26 0x00007ffff7c5b62c in vm_sendish (method_explorer=<optimized out>, block_handler=<optimized out>, cd=<optimized out>, reg_cfp=<optimized out>, ec=<optimized out>)
    at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm_insnhelper.c:55
81
#27 vm_exec_core (ec=0x55555555d1c0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/redhat-linux-build/insns.def:822
#28 0x00007ffff7c73bfe in vm_exec_loop (result=<optimized out>, tag=0x7ffffffffffd480, state=<optimized out>, ec=0x55555555d1c0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm.c:2499
#29 rb_vm_exec (ec=0x55555555d1c0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm.c:2478
#30 0x00007ffff7b358fb in require_internal (ec=ec@entry=0x55555555d1c0, fname=<optimized out>, fname@entry=140736888126320, exception=exception@entry=1, warn=false)
    at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/load.c:1247
#31 0x00007ffff7b35e4e in rb_require_string_internal (fname=140736888126320) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/load.c:1346
#32 0x00007ffff7b35f08 in rb_require_string (fname=<optimized out>) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/load.c:1339
#33 0x00007ffff7c540c7 in vm_call_cfunc_with_frame_ (ec=0x55555555d1c0, reg_cfp=0x7ffff7670e18, calling=<optimized out>, argc=<optimized out>, argv=<optimized out>, stack_bottom=<optimized out>)
    at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm_insnhelper.c:35
03
#34 0x00007ffff7c57b1f in vm_call_alias (ec=0x55555555d1c0, cfp=0x7ffff7670e18, calling=0x7ffffffffff

```

```

d9e0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm_insnhelper.c:
3873
#35 0x00007ffff7c5b62c in vm_sendish (method_explorer=<optimized out>, block_handler=<optimized ou
t>, cd=<optimized out>, reg_cfp=<optimized out>, ec=<optimized out>)
    at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm_insnhelper.c:55
81
--Type <RET> for more, q to quit, c to continue without paging--
#36 vm_exec_core (ec=0x55555555d1c0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.f
c40.285.x86_64/redhat-linux-build/insns.def:822
#37 0x00007ffff7c739dd in rb_vm_exec (ec=0x55555555d1c0) at /usr/src/debug/ruby-3.3.0~20231108.014
3gitc8d4b103a9-183.fc40.285.x86_64/vm.c:2472
#38 0x00007ffff7b358fb in require_internal (ec=ec@entry=0x55555555d1c0, fname=<optimized out>, fna
me@entry=140736882997040, exception=exception@entry=1, warn=false)
    at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/load.c:1247
#39 0x00007ffff7b35e4e in rb_require_string_internal (fname=140736882997040) at /usr/src/debug/rub
y-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/load.c:1346
#40 0x00007ffff7b35f08 in rb_require_string (fname=<optimized out>) at /usr/src/debug/ruby-3.3.0~2
0231108.0143gitc8d4b103a9-183.fc40.285.x86_64/load.c:1339
#41 0x00007ffff7c540c7 in vm_call_cfunc_with_frame_ (ec=0x55555555d1c0, reg_cfp=0x7ffff7670ec0, ca
lling=<optimized out>, argc=<optimized out>, argv=<optimized out>, stack_bottom=<optimized out>)
    at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm_insnhelper.c:35
03
#42 0x00007ffff7c57193 in vm_call_alias (calling=0x7ffffffffffe040, cfp=0x7ffff7670ec0, ec=0x55555555
d1c0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm_insnhelper.c:
3873
#43 vm_call_method_each_type (ec=0x55555555d1c0, cfp=0x7ffff7670ec0, calling=0x7ffffffffffe040) at /u
sr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm_insnhelper.c:4475
#44 0x00007ffff7c5b62c in vm_sendish (method_explorer=<optimized out>, block_handler=<optimized ou
t>, cd=<optimized out>, reg_cfp=<optimized out>, ec=<optimized out>)
    at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/vm_insnhelper.c:55
81
#45 vm_exec_core (ec=0x55555555d1c0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.f
c40.285.x86_64/redhat-linux-build/insns.def:822
#46 0x00007ffff7c73bfe in vm_exec_loop (result=<optimized out>, tag=0x7ffffffffffe0d0, state=<optimiz
ed out>, ec=0x55555555d1c0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x
86_64/vm.c:2499
#47 rb_vm_exec (ec=0x55555555d1c0) at /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc4
0.285.x86_64/vm.c:2478
#48 0x00007ffff7adbc0a in rb_ec_exec_node (ec=ec@entry=0x55555555d1c0, n=n@entry=0x7ffffdc3de580) a
t /usr/src/debug/ruby-3.3.0~20231108.0143gitc8d4b103a9-183.fc40.285.x86_64/eval.c:287
#49 0x00007ffff7adbd03 in ruby_run_node (n=0x7ffffdc3de580) at /usr/src/debug/ruby-3.3.0~20231108.0
143gitc8d4b103a9-183.fc40.285.x86_64/eval.c:328
#50 0x0000555555555197 in rb_main (argv=0x7ffffffffffe4a8, argc=2) at /usr/src/debug/ruby-3.3.0~20231
108.0143gitc8d4b103a9-183.fc40.285.x86_64/main.c:39
#51 main (argc=<optimized out>, argv=<optimized out>) at /usr/src/debug/ruby-3.3.0~20231108.0143gi
tc8d4b103a9-183.fc40.285.x86_64/main.c:58
(gdb) p cfunc
$1 = (const rb_method_cfunc_t *) 0xb
(gdb) deta
Detaching from program: /usr/bin/ruby-mri, process 345
/usr/share/rubygems/rubygems.rb:1220: [BUG] Segmentation fault at 0x000000000000001b
ruby 3.3.0dev (2023-11-08 master c8d4b103a9) [x86_64-linux]

-- Control frame information -----
c:0022 p:---- s:0126 e:000125 CFUNC
c:0021 p:0007 s:0123 e:000120 METHOD /usr/share/rubygems/rubygems.rb:1220
c:0020 p:0015 s:0115 e:000114 BLOCK <internal:/usr/share/rubygems/rubygems/core_ext/kernel_requir
e.rb>:42 [FINISH]
c:0019 p:---- s:0104 e:000103 [Inferior 1 (process 345) detached]
CFUNC :synchronize
c:0018 p:0017 s:0100 e:000099 METHOD <internal:/usr/share/rubygems/rubygems/core_ext/kernel_requir
e.rb>:39
c:0017 p:0006 s:0094 e:000093 TOP /usr/share/gems/gems/sqlite3-1.6.1/lib/sqlite3/pragmas.rb:1 [
FINISH]
c:0016 p:---- s:0091 e:000090 CFUNC :require
c:0015 p:0023 s:0086 e:000085 METHOD <internal:/usr/share/rubygems/rubygems/core_ext/kernel_requir
e.rb>:128

```

```

c:0014 p:0020 s:0080 e:000079 TOP      /usr/share/gems/gems/sqlite3-1.6.1/lib/sqlite3/database.rb:3
[FINISH]
c:0013 p:---- s:0077 e:000076 CFUNC    :require
c:0012 p:0023 s:0072 e:000071 METHOD    <internal:/usr/share/rubygems/rubygems/core_ext/kernel_require.rb>:128
c:0011 p:0033 s:0066 e:000065 TOP      /usr/share/gems/gems/sqlite3-1.6.1/lib/sqlite3.rb:9 [FINISH]
c:0010 p:---- s:0063 e:000062 CFUNC    :require
c:0009 p:0023 s:0058 e:000057 METHOD    <internal:/usr/share/rubygems/rubygems/core_ext/kernel_require.rb>:128
c:0008 p:0078 s:0052 e:000051 TOP      /usr/share/gems/gems/activerecord-7.0.8/lib/active_record/connection_adapters/sqlite3_adapter.rb:14 [FINISH]
c:0007 p:---- s:0049 e:000048 CFUNC    :require
c:0006 p:0023 s:0044 e:000043 METHOD    <internal:/usr/share/rubygems/rubygems/core_ext/kernel_require.rb>:128
c:0005 p:0051 s:0038 e:000037 METHOD    /usr/share/gems/gems/activerecord-7.0.8/lib/active_record/connection_adapters/abstract/connection_handler.rb:268
c:0004 p:0066 s:0027 e:000026 METHOD    /usr/share/gems/gems/activerecord-7.0.8/lib/active_record/connection_adapters/abstract/connection_handler.rb:129
c:0003 p:0049 s:0013 e:000012 METHOD    /usr/share/gems/gems/activerecord-7.0.8/lib/active_record/connection_handling.rb:52
c:0002 p:0020 s:0006 e:000005 EVAL     ./trial.rb:4 [FINISH]
c:0001 p:0000 s:0003 E:0018a0 DUMMY    [FINISH]

```

```

-- Ruby level backtrace information -----
./trial.rb:4:in `<main>'
/usr/share/gems/gems/activerecord-7.0.8/lib/active_record/connection_handling.rb:52:in `establish_connection'
/usr/share/gems/gems/activerecord-7.0.8/lib/active_record/connection_adapters/abstract/connection_handler.rb:129:in `establish_connection'
/usr/share/gems/gems/activerecord-7.0.8/lib/active_record/connection_adapters/abstract/connection_handler.rb:268:in `resolve_pool_config'
<internal:/usr/share/rubygems/rubygems/core_ext/kernel_require.rb>:128:in `require'
<internal:/usr/share/rubygems/rubygems/core_ext/kernel_require.rb>:128:in `require'
/usr/share/gems/gems/activerecord-7.0.8/lib/active_record/connection_adapters/sqlite3_adapter.rb:14:in `<top (required)>'
<internal:/usr/share/rubygems/rubygems/core_ext/kernel_require.rb>:128:in `require'
<internal:/usr/share/rubygems/rubygems/core_ext/kernel_require.rb>:128:in `require'
/usr/share/gems/gems/sqlite3-1.6.1/lib/sqlite3.rb:9:in `<top (required)>'
<internal:/usr/share/rubygems/rubygems/core_ext/kernel_require.rb>:128:in `require'
<internal:/usr/share/rubygems/rubygems/core_ext/kernel_require.rb>:128:in `require'
/usr/share/gems/gems/sqlite3-1.6.1/lib/sqlite3/database.rb:3:in `<top (required)>'
<internal:/usr/share/rubygems/rubygems/core_ext/kernel_require.rb>:128:in `require'
<internal:/usr/share/rubygems/rubygems/core_ext/kernel_require.rb>:128:in `require'
/usr/share/gems/gems/sqlite3-1.6.1/lib/sqlite3/pragmas.rb:1:in `<top (required)>'
<internal:/usr/share/rubygems/rubygems/core_ext/kernel_require.rb>:39:in `require'
<internal:/usr/share/rubygems/rubygems/core_ext/kernel_require.rb>:39:in `synchronize'
<internal:/usr/share/rubygems/rubygems/core_ext/kernel_require.rb>:42:in `block in require'
/usr/share/rubygems/rubygems.rb:1220:in `find_unresolved_default_spec'

```

Looks like cfunc points to invalid address. Currently I am unable to minimize the code further...

## Associated revisions

Revision [e201b81f79828c30500947fe8c8ea3c515e3d112](#) - 11/24/2023 06:16 PM - KJ Tsanaksidis

Mark cc->cme\_ for refinement callcaches as well

This is required for the same reason that super CC needs it.  
See [36023d5cb751d62fca0c27901c07527b20170f4d](#).

Reproducer:

```
def cached_foo_callsite(obj) = obj.foo
```

```
class Foo
  def foo = :v1
```

```
  module R
    refine Foo do
```

```

    def foo = :unused
  end
end
end

obj = Foo.new
cached_foo_callsite(obj) # set up cc with cme for foo=:v1

class Foo
  def foo = :v2
end
GC.start # cme for foo=:v1 collected, if not reachable by cached_foo_callsite

cached_foo_callsite(obj)

```

[Bug #19994]

#### Revision e201b81f79828c30500947fe8c8ea3c515e3d112 - 11/24/2023 06:16 PM - KJ Tsanaktsidis

Mark cc->cme\_ for refinement callccaches as well

This is required for the same reason that super CC needs it.  
See 36023d5cb751d62fca0c27901c07527b20170f4d.

Reproducer:

```

def cached_foo_callsite(obj) = obj.foo

class Foo
  def foo = :v1

  module R
    refine Foo do
      def foo = :unused
    end
  end
end

obj = Foo.new
cached_foo_callsite(obj) # set up cc with cme for foo=:v1

class Foo
  def foo = :v2
end
GC.start # cme for foo=:v1 collected, if not reachable by cached_foo_callsite

cached_foo_callsite(obj)

```

[Bug #19994]

#### Revision e201b81f - 11/24/2023 06:16 PM - KJ Tsanaktsidis

Mark cc->cme\_ for refinement callccaches as well

This is required for the same reason that super CC needs it.  
See 36023d5cb751d62fca0c27901c07527b20170f4d.

Reproducer:

```

def cached_foo_callsite(obj) = obj.foo

class Foo
  def foo = :v1

  module R
    refine Foo do
      def foo = :unused
    end
  end
end

obj = Foo.new
cached_foo_callsite(obj) # set up cc with cme for foo=:v1

class Foo

```

```
def foo = :v2
end
GC.start # cme for foo=:v1 collected, if not reachable by cached_foo_callsite

cached_foo_callsite(obj)
```

[Bug #19994]

#### Revision aecbd66742f43ccfcac04ca4143fcc68ad834320 - 12/10/2023 06:00 AM - KJ Tsanaksidis

Add RUBY\_ATOMIC\_{PTR\_,}FETCH macros for atomic loads

This can already be emulated by doing an atomic fetch\_add of zero, but this is more explicit.

[Bug #19994]

#### Revision aecbd66742f43ccfcac04ca4143fcc68ad834320 - 12/10/2023 06:00 AM - KJ Tsanaksidis

Add RUBY\_ATOMIC\_{PTR\_,}FETCH macros for atomic loads

This can already be emulated by doing an atomic fetch\_add of zero, but this is more explicit.

[Bug #19994]

#### Revision aecbd667 - 12/10/2023 06:00 AM - KJ Tsanaksidis

Add RUBY\_ATOMIC\_{PTR\_,}FETCH macros for atomic loads

This can already be emulated by doing an atomic fetch\_add of zero, but this is more explicit.

[Bug #19994]

## History

### #1 - 11/10/2023 06:51 AM - kjtsanaksidis (KJ Tsanaksidis)

So, I was able to reproduce this and bisect it, and found that <https://github.com/ruby/ruby/commit/4f0d58260a7f506ead198064d12a967edd11fe5e> was the commit that made your reproduction start crashing. That change *looks* correct to me, however, so I wonder if it's just the thing that shuffled the memory corruption around enough to make your script crash.

There definitely *is* some memory corruption; the cc->cme structure being called when the crash happens is all wrong. It's ->def member is just 0x1, the called\_id member is 10, and its defined\_class is rb\_cString (even though the method being called is on a Hash; the line of Ruby code being crashed on is default\_spec = @path\_to\_default\_spec\_map[path]).

My next step to debug this was to try building with ASAN, but I guess there's something about that which is not working currently; following the instructions I get a build which crashes immediately:

```
kj@kj-thinkpad ruby % ./miniruby -e 'puts "hi"'
=====
==990089==ERROR: AddressSanitizer: use-after-poison on address 0x7f43a6e0ba28 at pc 0x559111164462 bp 0x7ffc07e18780 sp 0x7ffc07e18778
READ of size 8 at 0x7f43a6e0ba28 thread T0
#0 0x559111164461 in RB_FL_TEST_RAW /home/kj/ruby/./include/ruby/internal/fl_type.h:472:25
#1 0x559111173749 in RB_ENCODING_GET_INLINED /home/kj/ruby/./include/ruby/internal/encoding/encoding.h:100
:17
#2 0x5591111635c4 in RB_ENCODING_GET /home/kj/ruby/./include/ruby/internal/encoding/encoding.h:196:20
#3 0x559111195bc0 in str_enc_copy /home/kj/ruby/string.c:722:28
#4 0x55911116d44c in rb_enc_cr_str_copy_for_substr /home/kj/ruby/string.c:745:5
#5 0x55911116f3d5 in rb_str_subseq /home/kj/ruby/string.c:2866:5
#6 0x559110f89408 in lex_get_str /home/kj/ruby/parse.y:7472:12
#7 0x559110f8bd83 in lex_getline /home/kj/ruby/parse.y:7478:18
#8 0x559110f8b601 in nextline /home/kj/ruby/parse.y:7655:40
#9 0x559110f8b0ad in nextc0 /home/kj/ruby/parse.y:7700:13
#10 0x559110f8dbb0 in parser_yylex /home/kj/ruby/parse.y:10421:17
#11 0x559110f622db in yylex /home/kj/ruby/parse.y:11121:9
#12 0x559110f3712e in ruby_yyparse /home/kj/ruby/parse.c:10180:16
#13 0x559110f898bd in yycompile0 /home/kj/ruby/parse.y:7379:9
#14 0x55911132b742 in rb_suppress_tracing /home/kj/ruby/vm_trace.c:483:18
#15 0x559110f7553e in yycompile /home/kj/ruby/parse.y:7434:5
#16 0x559110f74ff4 in parser_compile_string /home/kj/ruby/parse.y:7495:12
#17 0x559110f74de7 in rb_ruby_parser_compile_string_path /home/kj/ruby/parse.y:7502:12
#18 0x559110f79586 in rb_parser_compile_string_path /home/kj/ruby/parse.y:15614:12
#19 0x559110befe8a in prelude_ast /home/kj/ruby/miniprelude.c:7344:21
```

```

#20 0x559110bef223 in rb_builtin_ast /home/kj/ruby/miniprelude.c:7371:16
#21 0x559110bf005b in builtin_iseq_load /home/kj/ruby/./mini_builtin.c:21:21
#22 0x559110beff3c in rb_load_with_builtin_functions /home/kj/ruby/./mini_builtin.c:64:29
#23 0x559110ed7276 in Init_builtin_rjit_c /home/kj/ruby/rjit_c.rbinc:6266:3
#24 0x559110e19f2d in rb_call_builtin_inits /home/kj/ruby/inits.c:107:5
#25 0x55911111ac10 in ruby_opt_init /home/kj/ruby/ruby.c:1786:5
#26 0x55911111514f in process_options /home/kj/ruby/ruby.c:2279:9
#27 0x559111112478 in ruby_process_options /home/kj/ruby/ruby.c:2965:12
#28 0x559110d850da in ruby_options /home/kj/ruby/eval.c:121:9
#29 0x559110bee936 in rb_main /home/kj/ruby/./main.c:39:26
#30 0x559110bee7b9 in main /home/kj/ruby/./main.c:58:12
#31 0x7f43a95edb89 in __libc_start_call_main /usr/src/debug/glibc-2.37-13.fc38.x86_64/csu/../sysdeps/nptl/libc_start_call_main.h:58:16
#32 0x7f43a95edc4a in __libc_start_main@GLIBC_2.2.5 /usr/src/debug/glibc-2.37-13.fc38.x86_64/csu/../csu/libc-start.c:360:3
#33 0x559110b18094 in _start (/home/kj/ruby/miniruby+0x145094) (BuildId: 06bb735c1c8b6a0b766ee06fb9c7f146cc924f51)

```

Address 0x7f43a6e0ba28 is a wild pointer inside of access range of size 0x00000000000008.

SUMMARY: AddressSanitizer: use-after-poison /home/kj/ruby/./include/ruby/internal/fl\_type.h:472:25 in RB\_FL\_TE\_ST\_RAW

I'll try and debug this further over the weekend and see if I get anywhere, but in the meanwhile maybe the bisection result is useful to someone.

## #2 - 11/10/2023 04:20 PM - kjtsanaktisid (KJ Tsanaktisid)

OK, I made a bit of progress - I was able to get the repro working with ASAN, and it spat out this likely looking memory error:

```

kj@kj-thinkpad ruby % installed~/bin/ruby ~/repro.rb
=====
==54413==ERROR: AddressSanitizer: use-after-poison on address 0x7f236e8cab0 at pc 0x55c143ff9e67 bp 0x7fffe44c1630 sp 0x7fffe44c1628
READ of size 8 at 0x7f236e8cab0 thread T0
#0 0x55c143ff9e66 in vm_search_method_fastpath /home/kj/ruby/./vm_insnhelper.c:2222:13
#1 0x55c143ff9e66 in vm_sendish /home/kj/ruby/./vm_insnhelper.c:5581:27
#2 0x55c14400801e in vm_exec_core /home/kj/ruby/insns.def:802:11
#3 0x55c143ffa612 in rb_vm_exec /home/kj/ruby/vm.c:2472:22
#4 0x55c14408b97e in invoke_block /home/kj/ruby/vm.c:1497:12
#5 0x55c14408adb5 in invoke_iseq_block_from_c /home/kj/ruby/vm.c:1567:16
#6 0x55c14408adb5 in invoke_block_from_c_bh /home/kj/ruby/vm.c:1585:20
#7 0x55c14402b062 in vm_yield_with_cref /home/kj/ruby/vm.c:1622:12
#8 0x55c144087d30 in vm_yield /home/kj/ruby/vm.c:1630:12
#9 0x55c144026199 in rb_yield_0 /home/kj/ruby/./vm_eval.c:1362:12
#10 0x55c1440262e0 in rb_yield /home/kj/ruby/./vm_eval.c:1378:16
#11 0x55c14425df1f in rb_ary_each /home/kj/ruby/array.c:2532:9
#12 0x55c14407d7e8 in ractor_safe_call_cfunc_0 /home/kj/ruby/./vm_insnhelper.c:3320:12
#13 0x55c1440608b8 in vm_call_cfunc_with_frame_ /home/kj/ruby/./vm_insnhelper.c:3504:11
#14 0x55c14406111a in vm_call_cfunc_with_frame /home/kj/ruby/./vm_insnhelper.c:3532:12
#15 0x55c143ff9f44 in vm_sendish /home/kj/ruby/./vm_insnhelper.c:5582:15
#16 0x55c14400801e in vm_exec_core /home/kj/ruby/insns.def:802:11
#17 0x55c143ffa612 in rb_vm_exec /home/kj/ruby/vm.c:2472:22
#18 0x55c14408b97e in invoke_block /home/kj/ruby/vm.c:1497:12
#19 0x55c14408adb5 in invoke_iseq_block_from_c /home/kj/ruby/vm.c:1567:16
#20 0x55c14408adb5 in invoke_block_from_c_bh /home/kj/ruby/vm.c:1585:20
#21 0x55c14402b062 in vm_yield_with_cref /home/kj/ruby/vm.c:1622:12
#22 0x55c14402b9dc in yield_under /home/kj/ruby/./vm_eval.c:1949:12
#23 0x55c14402b271 in specific_eval /home/kj/ruby/./vm_eval.c:1990:16
#24 0x55c14402e132 in rb_mod_module_eval_internal /home/kj/ruby/./vm_eval.c:2120:12
#25 0x55c14407d7af in ractor_safe_call_cfunc_m1 /home/kj/ruby/./vm_insnhelper.c:3313:12
#26 0x55c1440608b8 in vm_call_cfunc_with_frame_ /home/kj/ruby/./vm_insnhelper.c:3504:11
#27 0x55c14406111a in vm_call_cfunc_with_frame /home/kj/ruby/./vm_insnhelper.c:3532:12
#28 0x55c143ff9f44 in vm_sendish /home/kj/ruby/./vm_insnhelper.c:5582:15
#29 0x55c14400801e in vm_exec_core /home/kj/ruby/insns.def:802:11
#30 0x55c143ffa612 in rb_vm_exec /home/kj/ruby/vm.c:2472:22
#31 0x55c1440830de in vm_call0_body /home/kj/ruby/./vm_eval.c:229:20
#32 0x55c14402344f in vm_call0_cc /home/kj/ruby/./vm_eval.c:110:12
#33 0x55c144024d4b in rb_funcallv_scope /home/kj/ruby/./vm_eval.c:1065:16
#34 0x55c14401d4b0 in rb_funcallv /home/kj/ruby/./vm_eval.c:1080:12
#35 0x55c144025ac3 in rb_funcall /home/kj/ruby/./vm_eval.c:1137:12
#36 0x55c143b1f6da in rb_mod_include /home/kj/ruby/eval.c:1159:9
#37 0x55c14407d7af in ractor_safe_call_cfunc_m1 /home/kj/ruby/./vm_insnhelper.c:3313:12
#38 0x55c1440608b8 in vm_call_cfunc_with_frame_ /home/kj/ruby/./vm_insnhelper.c:3504:11
#39 0x55c14406111a in vm_call_cfunc_with_frame /home/kj/ruby/./vm_insnhelper.c:3532:12
#40 0x55c143ff9f44 in vm_sendish /home/kj/ruby/./vm_insnhelper.c:5582:15
#41 0x55c14400801e in vm_exec_core /home/kj/ruby/insns.def:802:11

```

```

#42 0x55c143ffa612 in rb_vm_exec /home/kj/ruby/vm.c:2472:22
#43 0x55c144036ecf in rb_iseq_eval /home/kj/ruby/vm.c:2727:11
#44 0x55c143c479e8 in load_iseq_eval /home/kj/ruby/load.c:739:5
#45 0x55c143c3f680 in require_internal /home/kj/ruby/load.c:1247:21
#46 0x55c143c3caf0 in rb_require_string_internal /home/kj/ruby/load.c:1346:18
#47 0x55c143c3c99b in rb_require_string /home/kj/ruby/load.c:1339:12
#48 0x55c143c3c808 in rb_f_require /home/kj/ruby/load.c:981:12
#49 0x55c14407d851 in ractor_safe_call_cfunc_l /home/kj/ruby/./vm_insnhelper.c:3327:12
#50 0x55c1440608b8 in vm_call_cfunc_with_frame_ /home/kj/ruby/./vm_insnhelper.c:3504:11
#51 0x55c14406111a in vm_call_cfunc_with_frame /home/kj/ruby/./vm_insnhelper.c:3532:12
#52 0x55c14405fab9 in vm_call_cfunc_other /home/kj/ruby/./vm_insnhelper.c:3558:16
#53 0x55c14404954a in vm_call_cfunc /home/kj/ruby/./vm_insnhelper.c:3640:12
#54 0x55c144047465 in vm_call_method_each_type /home/kj/ruby/./vm_insnhelper.c:4418:16
#55 0x55c14404ba9e in vm_call_alias /home/kj/ruby/./vm_insnhelper.c:3874:12
#56 0x55c143ff9f44 in vm_sendish /home/kj/ruby/./vm_insnhelper.c:5582:15
#57 0x55c1440085af in vm_exec_core /home/kj/ruby/insns.def:822:11
#58 0x55c143ffa612 in rb_vm_exec /home/kj/ruby/vm.c:2472:22
#59 0x55c1440830de in vm_call0_body /home/kj/ruby/./vm_eval.c:229:20
#60 0x55c14402344f in vm_call0_cc /home/kj/ruby/./vm_eval.c:110:12
#61 0x55c144024d4b in rb_funcallv_scope /home/kj/ruby/./vm_eval.c:1065:16
#62 0x55c14401d4b0 in rb_funcallv /home/kj/ruby/./vm_eval.c:1080:12
#63 0x55c144025ac3 in rb_funcall /home/kj/ruby/./vm_eval.c:1137:12
#64 0x55c143ff0663 in autoload_feature_require /home/kj/ruby/variable.c:2898:20
#65 0x55c143fe790f in autoload_try_load /home/kj/ruby/variable.c:2912:20
#66 0x55c143b1da61 in rb_ensure /home/kj/ruby/eval.c:1009:18
#67 0x55c143fe6e3d in rb_autoload_load /home/kj/ruby/variable.c:2973:20
#68 0x55c143ff1a5f in rb_const_search_from /home/kj/ruby/variable.c:3075:17
#69 0x55c143fda9b7 in rb_const_search /home/kj/ruby/variable.c:3097:13
#70 0x55c143fe8660 in rb_const_get_0 /home/kj/ruby/variable.c:3024:15
#71 0x55c143fe87f8 in rb_public_const_get_from /home/kj/ruby/variable.c:3126:12
#72 0x55c143ff5654 in vm_get_ev_const /home/kj/ruby/./vm_insnhelper.c:1100:20
#73 0x55c143ffc68d in vm_get_ev_const_chain /home/kj/ruby/./vm_insnhelper.c:1124:15
#74 0x55c143ffc45f in rb_vm_opt_getconstant_path /home/kj/ruby/./vm_insnhelper.c:5890:15
#75 0x55c143fffbe9 in vm_exec_core /home/kj/ruby/insns.def:263:11
#76 0x55c144036de4 in vm_exec_loop /home/kj/ruby/vm.c:2499:22
#77 0x55c143ffa698 in rb_vm_exec /home/kj/ruby/vm.c:2478:18
#78 0x55c14403725f in rb_iseq_eval_main /home/kj/ruby/vm.c:2738:11
#79 0x55c143b19791 in rb_ec_exec_node /home/kj/ruby/eval.c:287:9
#80 0x55c143b191bb in ruby_run_node /home/kj/ruby/eval.c:328:30
#81 0x55c143b119bc in rb_main /home/kj/ruby/./main.c:39:12
#82 0x55c143b117c9 in main /home/kj/ruby/./main.c:58:12
#83 0x7f23d4a01b89 in __libc_start_call_main /usr/src/debug/glibc-2.37-13.fc38.x86_64/csu/./sysdeps/nptl/
libc_start_call_main.h:58:16
#84 0x7f23d4a01c4a in __libc_start_main@GLIBC_2.2.5 /usr/src/debug/glibc-2.37-13.fc38.x86_64/csu/./csu/li
bc-start.c:360:3
#85 0x55c143a3b0a4 in _start (/home/kj/ruby/installed~/bin/ruby+0x1440a4) (BuildId: d2084514ac5692bc3b08bd
a30312213a34a043bb)

```

Address 0x7f236e8cab0 is a wild pointer inside of access range of size 0x00000000000008.

SUMMARY: AddressSanitizer: use-after-poison /home/kj/ruby/./vm\_insnhelper.c:2222:13 in vm\_search\_method\_fastpa  
th

Shadow bytes around the buggy address:

```

0x7f236e8ca900: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x7f236e8ca980: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x7f236e8caa00: 00 00 00 00 00 00 00 00 00 00 00 00 00 f7 00 00 00
0x7f236e8caa80: f7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x7f236e8cab00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x7f236e8cab80: 00 00 00 00 00 00 00 00 00[f7]00 00 00 00 00 00 00
0x7f236e8cac00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x7f236e8cac80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x7f236e8cad00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x7f236e8cad80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x7f236e8cae00: 00 00 00 f7 00 00 00 00 f7 00 00 00 00 00 00 00

```

Shadow byte legend (one shadow byte represents 8 application bytes):

```

Addressable:                00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:          fa
Freed heap region:         fd
Stack left redzone:        f1
Stack mid redzone:         f2
Stack right redzone:       f3
Stack after return:        f5
Stack use after scope:     f8
Global redzone:            f9
Global init order:         f6

```



```
Poisoned by user:      f7
Container overflow:    fc
Array cookie:         ac
Intra object redzone: bb
ASan internal:        fe
Left alloca redzone:  ca
Right alloca redzone: cb
==54413==ABORTING
zsh: IOT instruction (core dumped)  installed~/bin/ruby ~/repro.rb
```

I should be able to tug on this a bit more in the next couple of days.

### #3 - 11/11/2023 06:13 AM - kjtsanaktsidis (KJ Tsanaktsidis)

I think I understand-ish the issue now and it looks like <https://github.com/ruby/ruby/pull/8899> fixes it (on my machine).

@mtasaka would you be able to tell me if this fixes the issue for you?

And [@ko1 \(Koichi Sasada\)](#) would you be able to look at my PR? I'm not very confident with the whole method resolution & caching machinery.

### #4 - 11/11/2023 06:56 AM - nobu (Nobuyoshi Nakada)

kjtsanaktsidis (KJ Tsanaktsidis) wrote in [#note-2](#):

OK, I made a bit of progress - I was able to get the repro working with ASAN, and it spat out this likely looking memory error:

```
kj@kj-thinkpad ruby % installed~/bin/ruby ~/repro.rb
```

What is the repro code?

Is it possible to add a test case?

### #5 - 11/11/2023 08:10 AM - kjtsanaktsidis (KJ Tsanaktsidis)

I was just using the reproduction code from the OP - I'm still trying to work out something minimal that can be checked in as a test which doesn't involve sqlite3 or activerecord. I did at least work out the reason test/unit is needed to make the crash happen - it requires `power_assert/enable_tracepoint_events` which defines refinements on a bunch of core classes. I don't have a complete unit-testable reproduction yet unfortunately.

I'm going to do a bit more work on the ASAN setup in ruby - I'm hoping that'll help lead me towards a more minimal case.

### #6 - 11/12/2023 03:20 AM - mtasaka (Mamoru TASAKA)

kjtsanaktsidis (KJ Tsanaktsidis) wrote in [#note-3](#):

@mtasaka would you be able to tell me if this fixes the issue for you?

Okay, with [e6916f1305](#) I still see this segfault, but with PR8899 applied, I don't see this segfault any longer and the original rubygem-stringex test suite also passes with PR8899 applied. Thank you!

### #7 - 11/24/2023 06:16 PM - Anonymous

- Status changed from Open to Closed

Applied in changeset [git!e201b81f79828c30500947fe8c8ea3c515e3d112](#).

---

Mark `cc->cme_` for refinement callcaches as well

This is required for the same reason that super CC needs it.  
See 36023d5cb751d62fca0c27901c07527b20170f4d.

Reproducer:

```
def cached_foo_callsite(obj) = obj.foo

class Foo
  def foo = :v1

  module R
    refine Foo do
      def foo = :unused
    end
  end
end
```

```
end

obj = Foo.new
cached_foo_callsite(obj) # set up cc with cme for foo=:v1

class Foo
  def foo = :v2
end
GC.start # cme for foo=:v1 collected, if not reachable by cached_foo_callsite

cached_foo_callsite(obj)

[Bug #19994]
```