

Ruby - Bug #21206

Segmentation fault on ISeq#to_binary

03/31/2025 02:39 AM - shyouhei (Shyouhei Urabe)

Status:	Open	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 3.4.2 (2025-02-15 revision d2930f8e7a) +PRISM +GC [aarch64-linux-gnu]	Backport: 3.1: UNKNOWN, 3.2: UNKNOWN, 3.3: UNKNOWN, 3.4: UNKNOWN

Description

Found this SEGV using bootsnap.

This could well be architecture dependent because of ISeqs being so by nature.

Also this doesn't happen when the ISeq is created using compile_prism.

```
$ ruby -ve 'RubyVM::InstructionSequence.compile_parsey("def f(g) = each {nil rescue g+it}).to_binary'
ruby 3.4.2 (2025-02-15 revision d2930f8e7a) +PRISM +GC [aarch64-linux-gnu]
-e:1: [BUG] Segmentation fault at 0x0000000000000000
ruby 3.4.2 (2025-02-15 revision d2930f8e7a) +PRISM +GC [aarch64-linux-gnu]

-- Control frame information -----
c:0003 p:---- s:0010 e:000009 CFUNC :to_binary
c:0002 p:0008 s:0006 e:000005 EVAL -e:1 [FINISH]
c:0001 p:0000 s:0003 E:000190 DUMMY [FINISH]

-- Ruby level backtrace information -----
-e:1:in '<main>'
-e:1:in 'to_binary'

-- Threading information -----
Total ractor count: 1
Ruby thread count for this ractor: 1

-- Machine register context -----
 x0: 0x0000000000000000 x1: 0x0000ffff8a15d0a8 x2: 0x0000000000000000
 x3: 0x0000000000000003 x4: 0x0000000000000000 x5: 0x0000ffffa4346b50
 x6: 0x0000000000000005 x7: 0x00000000fffffffffe x18: 0x000000000116810c
x19: 0x0000ffff8a15d0a8 x20: 0x0000000000000000 x21: 0x0000000000000001
x22: 0x0000ffffc0f0d968 x23: 0x0000ffffc0f0d4c0 x24: 0x0000000000000018
x25: 0x0000ffffa3c98530 x26: 0x0000000000000000 x27: 0x0000000000000002
x28: 0x0000ffffc0f0d4e8 x29: 0x0000ffffc0f0d410 sp: 0x0000ffffc0f0d410
fau: 0x0000000000000000

-- C level backtrace information -----
/lib/aarch64-linux-gnu/libruby-3.4.so.3.4(0xfffffa3e8ff84) [0xfffffa3e8ff84]
/lib/aarch64-linux-gnu/libruby-3.4.so.3.4(0xfffffa3e95514) [0xfffffa3e95514]
/lib/aarch64-linux-gnu/libruby-3.4.so.3.4(0xfffffa3ce760c) [0xfffffa3ce760c]
/lib/aarch64-linux-gnu/libruby-3.4.so.3.4(0xfffffa3e0de88) [0xfffffa3e0de88]
linux-vdso.so.1(__kernel_rt_sigreturn+0x0) [0xfffffa43447a0]
/lib/aarch64-linux-gnu/libruby-3.4.so.3.4(rb_str_cmp+0x24) [0xfffffa3e17d94]
[0xfffffa3980b9c]
[0xfffffa3980efc]
[0xfffffa3f418c8]
[0xfffffa3c98d4c]
[0xfffffa3da2484]
/lib/aarch64-linux-gnu/libruby-3.4.so.3.4(rb_st_foreach+0x44) [0xfffffa3e06944]
[0xfffffa3f213e4]
[0xfffffa3d46ea4]
```

```
[0xfffffa3e6c92c]
[0xfffffa3e767a8]
[0xfffffa3e8cae8]
[0xfffffa3ce6ac4]
/lib/aarch64-linux-gnu/libruby-3.4.so.3.4(ruby_run_node+0x9c) [0xfffffa3cebba0]
[0xaaaae2be0b30]
[0xfffffa39684c4]
[0xfffffa3968598]
[0xaaaae2be0bb0]
```

```
-- Other runtime information -----
```

```
* Loaded script: -e
```

```
* Loaded features:
```

```
 0 enumerator.so
 1 thread.rb
 2 fiber.so
 3 rational.so
 4 complex.so
 5 ruby2_keywords.rb
 6 /usr/lib/aarch64-linux-gnu/ruby/3.4.0/enc/encdb.so
 7 /usr/lib/aarch64-linux-gnu/ruby/3.4.0/enc/trans/transdb.so
 8 /usr/lib/aarch64-linux-gnu/ruby/3.4.0/rbconfig.rb
 9 /usr/lib/ruby/3.4.0/rubygems/compatibility.rb
10 /usr/lib/ruby/3.4.0/rubygems/defaults.rb
11 /usr/lib/ruby/3.4.0/rubygems/deprecate.rb
12 /usr/lib/ruby/3.4.0/rubygems/errors.rb
13 /usr/lib/ruby/3.4.0/rubygems/target_rbconfig.rb
14 /usr/lib/ruby/3.4.0/rubygems/unknown_command_spell_checker.rb
15 /usr/lib/ruby/3.4.0/rubygems/exceptions.rb
16 /usr/lib/ruby/3.4.0/rubygems/basic_specification.rb
17 /usr/lib/ruby/3.4.0/rubygems/stub_specification.rb
18 /usr/lib/ruby/3.4.0/rubygems/platform.rb
19 /usr/lib/ruby/3.4.0/rubygems/specification_record.rb
20 /usr/lib/ruby/3.4.0/rubygems/util/list.rb
21 /usr/lib/ruby/3.4.0/rubygems/version.rb
22 /usr/lib/ruby/3.4.0/rubygems/requirement.rb
23 /usr/lib/ruby/3.4.0/rubygems/specification.rb
24 /usr/lib/ruby/vendor_ruby/rubygems/defaults/operating_system.rb
25 /usr/lib/ruby/3.4.0/rubygems/util.rb
26 /usr/lib/ruby/3.4.0/rubygems/dependency.rb
27 /usr/lib/ruby/3.4.0/rubygems/core_ext/kernel_gem.rb
28 /usr/lib/aarch64-linux-gnu/ruby/3.4.0/monitor.so
29 /usr/lib/ruby/3.4.0/monitor.rb
30 /usr/lib/ruby/3.4.0/rubygems.rb
31 /usr/lib/ruby/3.4.0/bundled_gems.rb
32 /usr/lib/ruby/3.4.0/rubygems/path_support.rb
33 /usr/lib/ruby/3.4.0/error_highlight/version.rb
34 /usr/lib/ruby/3.4.0/error_highlight/base.rb
35 /usr/lib/ruby/3.4.0/error_highlight/formatter.rb
36 /usr/lib/ruby/3.4.0/error_highlight/core_ext.rb
37 /usr/lib/ruby/3.4.0/error_highlight.rb
38 /usr/lib/ruby/3.4.0/did_you_mean/version.rb
39 /usr/lib/ruby/3.4.0/did_you_mean/core_ext/name_error.rb
40 /usr/lib/ruby/3.4.0/did_you_mean/levenshtein.rb
41 /usr/lib/ruby/3.4.0/did_you_mean/jaro_winkler.rb
42 /usr/lib/ruby/3.4.0/did_you_mean/spell_checker.rb
43 /usr/lib/ruby/3.4.0/did_you_mean/spell_checkers/name_error_checkers/class_name_checker.rb
44 /usr/lib/ruby/3.4.0/did_you_mean/spell_checkers/name_error_checkers/variable_name_checker.rb
45 /usr/lib/ruby/3.4.0/did_you_mean/spell_checkers/name_error_checkers.rb
46 /usr/lib/ruby/3.4.0/did_you_mean/spell_checkers/method_name_checker.rb
47 /usr/lib/ruby/3.4.0/did_you_mean/spell_checkers/key_error_checker.rb
48 /usr/lib/ruby/3.4.0/did_you_mean/spell_checkers/null_checker.rb
49 /usr/lib/ruby/3.4.0/did_you_mean/tree_spell_checker.rb
50 /usr/lib/ruby/3.4.0/did_you_mean/spell_checkers/require_path_checker.rb
```

```
51 /usr/lib/ruby/3.4.0/did_you_mean/spell_checkers/pattern_key_name_checker.rb
52 /usr/lib/ruby/3.4.0/did_you_mean/formatter.rb
53 /usr/lib/ruby/3.4.0/did_you_mean.rb
54 /usr/lib/ruby/3.4.0/syntax_suggest/core_ext.rb
```

* Process memory map:

```
aaaae2be0000-aaaae2be1000 r-xp 00000000 00:34 763738 /usr/bin/ruby3.4
aaaae2bff000-aaaae2c00000 r--p 0000f000 00:34 763738 /usr/bin/ruby3.4
aaaae2c00000-aaaae2c01000 rw-p 00010000 00:34 763738 /usr/bin/ruby3.4
aaab18253000-aaab18545000 rw-p 00000000 00:00 0 [heap]
ffff87c00000-ffff881f3000 r--s 00000000 00:34 763745 /usr/lib/aarch64-linux-gn
u/libruby-3.4.so.3.4.2
ffff88200000-ffff88201000 ---p 00000000 00:00 0
ffff88201000-ffff882a2000 rw-p 00000000 00:00 0
ffff882a2000-ffff882a3000 ---p 00000000 00:00 0
ffff882a3000-ffff88344000 rw-p 00000000 00:00 0
ffff88344000-ffff88345000 ---p 00000000 00:00 0
ffff88345000-ffff883e6000 rw-p 00000000 00:00 0
ffff883e6000-ffff883e7000 ---p 00000000 00:00 0
ffff883e7000-ffff88488000 rw-p 00000000 00:00 0
ffff88488000-ffff88489000 ---p 00000000 00:00 0
ffff88489000-ffff8852a000 rw-p 00000000 00:00 0
ffff8852a000-ffff8852b000 ---p 00000000 00:00 0
ffff8852b000-ffff885cc000 rw-p 00000000 00:00 0
ffff885cc000-ffff885cd000 ---p 00000000 00:00 0
ffff885cd000-ffff8866e000 rw-p 00000000 00:00 0
ffff8866e000-ffff8866f000 ---p 00000000 00:00 0
ffff8866f000-ffff88710000 rw-p 00000000 00:00 0
ffff88710000-ffff88711000 ---p 00000000 00:00 0
ffff88711000-ffff887b2000 rw-p 00000000 00:00 0
ffff887b2000-ffff887b3000 ---p 00000000 00:00 0
ffff887b3000-ffff88854000 rw-p 00000000 00:00 0
ffff88854000-ffff88855000 ---p 00000000 00:00 0
ffff88855000-ffff888f6000 rw-p 00000000 00:00 0
ffff888f6000-ffff888f7000 ---p 00000000 00:00 0
ffff888f7000-ffff88998000 rw-p 00000000 00:00 0
ffff88998000-ffff88999000 ---p 00000000 00:00 0
ffff88999000-ffff88a3a000 rw-p 00000000 00:00 0
ffff88a3a000-ffff88a3b000 ---p 00000000 00:00 0
ffff88a3b000-ffff88adc000 rw-p 00000000 00:00 0
ffff88adc000-ffff88add000 ---p 00000000 00:00 0
ffff88add000-ffff88b7e000 rw-p 00000000 00:00 0
ffff88b7e000-ffff88b7f000 ---p 00000000 00:00 0
ffff88b7f000-ffff88c20000 rw-p 00000000 00:00 0
ffff88c20000-ffff88c21000 ---p 00000000 00:00 0
ffff88c21000-ffff88cc2000 rw-p 00000000 00:00 0
ffff88cc2000-ffff88cc3000 ---p 00000000 00:00 0
ffff88cc3000-ffff88d64000 rw-p 00000000 00:00 0
ffff88d64000-ffff88d65000 ---p 00000000 00:00 0
ffff88d65000-ffff88e06000 rw-p 00000000 00:00 0
ffff88e06000-ffff88e07000 ---p 00000000 00:00 0
ffff88e07000-ffff88ea8000 rw-p 00000000 00:00 0
ffff88ea8000-ffff88ea9000 ---p 00000000 00:00 0
ffff88ea9000-ffff88f4a000 rw-p 00000000 00:00 0
ffff88f4a000-ffff88f4b000 ---p 00000000 00:00 0
ffff88f4b000-ffff88fec000 rw-p 00000000 00:00 0
ffff88fec000-ffff88fed000 ---p 00000000 00:00 0
ffff88fed000-ffff8908e000 rw-p 00000000 00:00 0
ffff8908e000-ffff8908f000 ---p 00000000 00:00 0
ffff8908f000-ffff89130000 rw-p 00000000 00:00 0
ffff89130000-ffff89131000 ---p 00000000 00:00 0
ffff89131000-ffff891d2000 rw-p 00000000 00:00 0
ffff891d2000-ffff891d3000 ---p 00000000 00:00 0
ffff891d3000-ffff89274000 rw-p 00000000 00:00 0
ffff89274000-ffff89275000 ---p 00000000 00:00 0
ffff89275000-ffff89316000 rw-p 00000000 00:00 0
```

```

ffff89316000-ffff89317000 ---p 00000000 00:00 0
ffff89317000-ffff893b8000 rw-p 00000000 00:00 0
ffff893b8000-ffff893b9000 ---p 00000000 00:00 0
ffff893b9000-ffff8945a000 rw-p 00000000 00:00 0
ffff8945a000-ffff8945b000 ---p 00000000 00:00 0
ffff8945b000-ffff894fc000 rw-p 00000000 00:00 0
ffff894fc000-ffff894fd000 ---p 00000000 00:00 0
ffff894fd000-ffff8959e000 rw-p 00000000 00:00 0
ffff8959e000-ffff8959f000 ---p 00000000 00:00 0
ffff8959f000-ffff89640000 rw-p 00000000 00:00 0
ffff89800000-ffff89810000 ---p 00000000 00:00 0
ffff89810000-ffff8a010000 rw-p 00000000 00:00 0
ffff8a0d0000-ffff8a0e0000 rw-p 00000000 00:00 0
ffff8a0ef000-ffff8a120000 rw-p 00000000 00:00 0
ffff8a120000-ffff8a122000 r-xp 00000000 00:34 763838 /usr/lib/aarch64-linux-gn
u/ruby/3.4.0/monitor.so
ffff8a122000-ffff8a13f000 ---p 00002000 00:34 763838 /usr/lib/aarch64-linux-gn
u/ruby/3.4.0/monitor.so
ffff8a13f000-ffff8a140000 r--p 0000f000 00:34 763838 /usr/lib/aarch64-linux-gn
u/ruby/3.4.0/monitor.so
ffff8a140000-ffff8a141000 rw-p 00010000 00:34 763838 /usr/lib/aarch64-linux-gn
u/ruby/3.4.0/monitor.so
ffff8a150000-ffffa3600000 rw-p 00000000 00:00 0
ffffa3610000-ffffa36d0000 rw-p 00000000 00:00 0
ffffa36d0000-ffffa36d2000 r-xp 00000000 00:34 763811 /usr/lib/aarch64-linux-gn
u/ruby/3.4.0/enc/trans/transdb.so
ffffa36d2000-ffffa36ef000 ---p 00002000 00:34 763811 /usr/lib/aarch64-linux-gn
u/ruby/3.4.0/enc/trans/transdb.so
ffffa36ef000-ffffa36f0000 r--p 0000f000 00:34 763811 /usr/lib/aarch64-linux-gn
u/ruby/3.4.0/enc/trans/transdb.so
ffffa36f0000-ffffa36f1000 rw-p 00010000 00:34 763811 /usr/lib/aarch64-linux-gn
u/ruby/3.4.0/enc/trans/transdb.so
ffffa3700000-ffffa3710000 rw-p 00000000 00:00 0
ffffa3710000-ffffa3712000 r-xp 00000000 00:34 763767 /usr/lib/aarch64-linux-gn
u/ruby/3.4.0/enc/encdb.so
ffffa3712000-ffffa372f000 ---p 00002000 00:34 763767 /usr/lib/aarch64-linux-gn
u/ruby/3.4.0/enc/encdb.so
ffffa372f000-ffffa3730000 r--p 0000f000 00:34 763767 /usr/lib/aarch64-linux-gn
u/ruby/3.4.0/enc/encdb.so
ffffa3730000-ffffa3731000 rw-p 00010000 00:34 763767 /usr/lib/aarch64-linux-gn
u/ruby/3.4.0/enc/encdb.so
ffffa3740000-ffffa3790000 rw-p 00000000 00:00 0
ffffa379e000-ffffa3900000 rw-p 00000000 00:00 0
ffffa3900000-ffffa391f000 r-xp 00000000 00:34 566619 /usr/lib/aarch64-linux-gn
u/libgcc_s.so.1
ffffa391f000-ffffa392f000 ---p 0001f000 00:34 566619 /usr/lib/aarch64-linux-gn
u/libgcc_s.so.1
ffffa392f000-ffffa3930000 r--p 0001f000 00:34 566619 /usr/lib/aarch64-linux-gn
u/libgcc_s.so.1
ffffa3930000-ffffa3931000 rw-p 00020000 00:34 566619 /usr/lib/aarch64-linux-gn
u/libgcc_s.so.1
ffffa3940000-ffffa3ada000 r-xp 00000000 00:34 770271 /usr/lib/aarch64-linux-gn
u/libc.so.6
ffffa3ada000-ffffa3aed000 ---p 0019a000 00:34 770271 /usr/lib/aarch64-linux-gn
u/libc.so.6
ffffa3aed000-ffffa3af0000 r--p 0019d000 00:34 770271 /usr/lib/aarch64-linux-gn
u/libc.so.6
ffffa3af0000-ffffa3af2000 rw-p 001a0000 00:34 770271 /usr/lib/aarch64-linux-gn
u/libc.so.6
ffffa3af2000-ffffa3afe000 rw-p 00000000 00:00 0
ffffa3b00000-ffffa3b85000 r-xp 00000000 00:34 770303 /usr/lib/aarch64-linux-gn
u/libm.so.6
ffffa3b85000-ffffa3b9f000 ---p 00085000 00:34 770303 /usr/lib/aarch64-linux-gn
u/libm.so.6
ffffa3b9f000-ffffa3ba0000 r--p 0008f000 00:34 770303 /usr/lib/aarch64-linux-gn
u/libm.so.6
ffffa3ba0000-ffffa3ba1000 rw-p 00090000 00:34 770303 /usr/lib/aarch64-linux-gn

```

```

u/libm.so.6
ffffa3bb0000-ffffa3bdd000 r-xp 00000000 00:34 566603 /usr/lib/aarch64-linux-gn
u/libcrypt.so.1.1.0
ffffa3bdd000-ffffa3bef000 ---p 0002d000 00:34 566603 /usr/lib/aarch64-linux-gn
u/libcrypt.so.1.1.0
ffffa3bef000-ffffa3bf0000 r--p 0002f000 00:34 566603 /usr/lib/aarch64-linux-gn
u/libcrypt.so.1.1.0
ffffa3bf0000-ffffa3bf1000 rw-p 00030000 00:34 566603 /usr/lib/aarch64-linux-gn
u/libcrypt.so.1.1.0
ffffa3bf1000-ffffa3bf9000 rw-p 00000000 00:00 0
ffffa3c00000-ffffa41cb000 r-xp 00000000 00:34 763745 /usr/lib/aarch64-linux-gn
u/libruby-3.4.so.3.4.2
ffffa41cb000-ffffa41d6000 ---p 005cb000 00:34 763745 /usr/lib/aarch64-linux-gn
u/libruby-3.4.so.3.4.2
ffffa41d6000-ffffa41f0000 r--p 005d6000 00:34 763745 /usr/lib/aarch64-linux-gn
u/libruby-3.4.so.3.4.2
ffffa41f0000-ffffa41f1000 rw-p 005f0000 00:34 763745 /usr/lib/aarch64-linux-gn
u/libruby-3.4.so.3.4.2
ffffa41f1000-ffffa4206000 rw-p 00000000 00:00 0
ffffa420f000-ffffa4220000 r--s 00000000 00:34 763738 /usr/bin/ruby3.4
ffffa4220000-ffffa4230000 rw-p 00000000 00:00 0
ffffa4230000-ffffa42aa000 r-xp 00000000 00:34 767074 /usr/lib/aarch64-linux-gn
u/libgmp.so.10.5.0
ffffa42aa000-ffffa42bf000 ---p 0007a000 00:34 767074 /usr/lib/aarch64-linux-gn
u/libgmp.so.10.5.0
ffffa42bf000-ffffa42c0000 r--p 0007f000 00:34 767074 /usr/lib/aarch64-linux-gn
u/libgmp.so.10.5.0
ffffa42c0000-ffffa42c1000 rw-p 00080000 00:34 767074 /usr/lib/aarch64-linux-gn
u/libgmp.so.10.5.0
ffffa42d0000-ffffa42ea000 r-xp 00000000 00:34 566707 /usr/lib/aarch64-linux-gn
u/libz.so.1.3
ffffa42ea000-ffffa42ff000 ---p 0001a000 00:34 566707 /usr/lib/aarch64-linux-gn
u/libz.so.1.3
ffffa42ff000-ffffa4300000 r--p 0001f000 00:34 566707 /usr/lib/aarch64-linux-gn
u/libz.so.1.3
ffffa4300000-ffffa4301000 rw-p 00020000 00:34 566707 /usr/lib/aarch64-linux-gn
u/libz.so.1.3
ffffa4307000-ffffa432e000 r-xp 00000000 00:34 769991 /usr/lib/aarch64-linux-gn
u/ld-linux-aarch64.so.1
ffffa4339000-ffffa433d000 rw-p 00000000 00:00 0
ffffa4340000-ffffa4342000 rw-p 00000000 00:00 0
ffffa4342000-ffffa4344000 r--p 00000000 00:00 0 [vvar]
ffffa4344000-ffffa4345000 r-xp 00000000 00:00 0 [vdso]
ffffa4345000-ffffa4347000 r--p 0002e000 00:34 769991 /usr/lib/aarch64-linux-gn
u/ld-linux-aarch64.so.1
ffffa4347000-ffffa4349000 rw-p 00030000 00:34 769991 /usr/lib/aarch64-linux-gn
u/ld-linux-aarch64.so.1
ffffc0eef000-ffffc0f10000 rw-p 00000000 00:00 0 [stack]

```

Segmentation fault

History

#1 - 04/02/2025 01:26 PM - byroot (Jean Boussier)

Running in on ruby master with debugs run into the following assertion failure:

```

../include/ruby/internal/core/rstring.h:391: Assertion Failed: rbimpl_rstring_getmem:RB_TYPE_P(str, RUBY_T_STR
ING): actual type: 19

```

#2 - 04/02/2025 02:04 PM - byroot (Jean Boussier)

I tracked it down to:

```

    if (!p->it_id) {
        p->it_id = internal_id(p);
        vtable_add(p->lvtbl->args, p->it_id);
    }

```

Internal IDs can't be serialized.

It seems there was an attempt to fix this but it was reverted in <https://github.com/ruby/ruby/commit/667a0f9f928>