

Ruby - Bug #20727

YJIT segmentation fault inside of invalidate_block_version

09/12/2024 06:09 PM - jhawthorn (John Hawthorn)

Status:	Assigned	
Priority:	Normal	
Assignee:	jit	
Target version:		
ruby -v:		Backport: 3.1: UNKNOWN, 3.2: UNKNOWN, 3.3: UNKNOWN

Description

For a while we've been seeing an occasional segfault in production inside of YJIT's invalidation code. It seems to happen most often when a invalidation on a widely used CME.

```
[BUG] Segmentation fault at 0x0000000000000014"
"ruby 3.3.5 (2024-09-04 revision 4f143c3038) +YJIT [x86_64-linux]"
null
"-- Control frame information -----"
"c:0174 p:---- s:1247 e:001246 CFUNC :extend_object"
"c:0173 p:---- s:1244 e:001243 CFUNC :extend"
"c:0172 p:0049 s:1239 e:001238 METHOD /build/vendor/gems/3.3.5/ruby/3.3.0/gems/activerecord-8.0.0.alpha.6395186/lib/active_record/relation/query_methods.rb:1467"
"c:0171 p:0024 s:1233 e:001232 METHOD /build/vendor/gems/3.3.5/ruby/3.3.0/gems/activerecord-8.0.0.alpha.6395186/lib/active_record/relation/query_methods.rb:1456"
"c:0170 p:0055 s:1227 e:001226 METHOD /build/vendor/gems/3.3.5/ruby/3.3.0/gems/will_paginate-4.0.1/lib/will_paginate/active_record.rb:170"
"c:0169 p:0076 s:1219 e:001218 METHOD /build/vendor/gems/3.3.5/ruby/3.3.0/gems/will_paginate-4.0.1/lib/will_paginate/active_record.rb:154"
-----8<-----
null
"-- Threading information -----"
"Total ractor count: 1"
"Ruby thread count for this ractor: 19"
null
"-- Machine register context -----"
" RIP: 0x0000563c0aaccef7 RBP: 0x00007f481524f5f0 RSP: 0x00007fffe8631d70"
" RAX: 0x0000000000000014 RBX: 0x0000000000000010 RCX: 0x000000000000000e"
" RDX: 0x0000000002ff9bab RDI: 0x00007f4839357520 RSI: 0x0000000000000008"
"  R8: 0x00007f480cc0f5e0  R9: 0x0000000000000800 R10: 0x00007f48af4008c0"
" R11: 0x0000000000000060 R12: 0x0000563c0ad93108 R13: 0x00007f4816abe260"
" R14: 0x000000000000000e R15: 0x0000000002f9d50f EFL: 0x0000000000010206"
null
"-- C level backtrace information -----"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(rb_print_backtrace+0x11) [0x563c0a9ff8df] vm_dump.c:820"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(rb_vm_bugreport) vm_dump.c:151"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(rb_bug_for_fatal_signal+0xfc) [0x563c0abc2a1c] error.c:1065"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(sigsegv+0x4d) [0x563c0a94e02d] signal.c:926"
"/lib/x86_64-linux-gnu/libpthread.so.0(__restore_rt+0x0) [0x7f48afb1420]"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(0x563c0aaccef7) [0x563c0aaccef7]"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby({closure#0}) yjit/src/core.rs:718"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(invalidate_block_version) yjit/src/core.rs:3237"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby({closure#0}+0xe6) [0x563c0aaf1586] yjit/src/invariants.rs:246"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(do_call<yjit::invariants::rb_yjit_cme_invalidate::{closure_env#0}, ()>) /rustc/07dca489ac2d933c78d3c5158e3f43beefeb02ce/librar
```

```

y/std/src/panicking.rs:552"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(try<(), yjit::invariants::rb_yjit_cme_invalidate::{closure_env#0}>) /rustc/07dca489ac2d933c78d3c5158e3f43beefeb02ce/library/std/src/panicking.rs:516"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(catch_unwind<yjit::invariant s::rb_yjit_cme_invalidate::{closure_env#0}, ()>+0x8) [0x563c0aae2d68] /rustc/07dca489ac2d933c78d3c5158e3f43beefeb02ce/library/s>
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(with_vm_lock<yjit::invariant s::rb_yjit_cme_invalidate::{closure_env#0}, ()>) yjit/src/cruby.rs:646"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(rb_yjit_cme_invalidate+0x5c) [0x563c0aae6e0c] yjit/src/invariants.rs:243"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(vm_cme_invalidate+0x12) [0x563c0a9d78bd] vm_method.c:126"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(clear_method_cache_by_id_in_class) vm_method.c:240"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(clear_module_cache_i+0x13) [0x563c0ab2d263] class.c:1234"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(rb_id_table_foreach+0x84) [0x563c0a9891c4] id_table.c:278"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(do_include_modules_at+0x16a) [0x563c0ab31a0a] class.c:1314"
"/build/vendor/ruby/4f143c30380724f14341665b622148b0646138fe/bin/ruby(include_modules_at+0x1a) [0x563c0ab31f61] class.c:1370"
-----8<-----

```

History

#1 - 09/13/2024 03:47 AM - k0kubun (Takashi Kokubun)

- Assignee set to jit

#2 - 09/20/2024 12:27 AM - hsbt (Hiroshi SHIBATA)

- Status changed from Open to Assigned

#3 - 02/18/2025 04:29 PM - froydnj (Nathan Froyd)

We are seeing this in 3.3.4 and 3.3.5, but it is coming from `rb_yjit_constant_state_changed`, e.g.:

```

ruby: YJIT has panicked. More info to follow...
thread '<unnamed>' panicked at ./yjit/src/core.rs:3246:87:
called
Option::unwrap()
  on a
None
  value
stack backtrace:
 0: rust_begin_unwind
   at /rustc/82e1608dfa6e0b5569232559e3d385fea5a93112/library/std/src/panicking.rs:645:5
 1: core::panicking::panic_fmt
   at /rustc/82e1608dfa6e0b5569232559e3d385fea5a93112/library/core/src/panicking.rs:72:14
 2: core::panicking::panic
   at /rustc/82e1608dfa6e0b5569232559e3d385fea5a93112/library/core/src/panicking.rs:127:5
 3: core::option::Option<T>::unwrap
   at /rustc/82e1608dfa6e0b5569232559e3d385fea5a93112/library/core/src/option.rs:931:21
 4: yjit::core::invalidate_block_version
   at /tmp/tmp.tcdXUumPig/yjit/src/core.rs:3246:87
 5: yjit::invariants::rb_yjit_constant_state_changed::{closure}
   at /tmp/tmp.tcdXUumPig/yjit/src/invariants.rs:286:17
 6: std::panicking::try::do_call
   at /rustc/82e1608dfa6e0b5569232559e3d385fea5a93112/library/std/src/panicking.rs:552:40
 7: std::panicking::try
   at /rustc/82e1608dfa6e0b5569232559e3d385fea5a93112/library/std/src/panicking.rs:516:19
 8: std::panic::catch_unwind
   at /rustc/82e1608dfa6e0b5569232559e3d385fea5a93112/library/std/src/panic.rs:142:14
 9: yjit::cruby::with_vm_lock
   at /tmp/tmp.tcdXUumPig/yjit/src/cruby.rs:646:21
10: rb_yjit_constant_state_changed
   at /tmp/tmp.tcdXUumPig/yjit/src/invariants.rs:282:5
11: rb_clear_constant_cache_for_id
   at /tmp/tmp.tcdXUumPig/vm_method.c:152:5
12: const_tbl_update

```

```
      at /tmp/tmp.tcdXUumPig/variable.c:3672:9
13: const_set
      at /tmp/tmp.tcdXUumPig/variable.c:3561:13
14: rb_const_set
      at /tmp/tmp.tcdXUumPig/variable.c:3598:5
```

Looking at the instances where this occurs, it seems to be with gems defining their own, namespaced String constant.