Ruby - Bug #19103

[3.2.0dev] [BUG] Segmentation fault at 0x0000000000000000 in rgengc_check_relation

11/04/2022 11:23 AM - byroot (Jean Boussier)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 3.2.0dev (2022-10-19T19:36:24Z master 0d360ee7ff)	**Backport:**	2.7: UNKNOWN, 3.0: UNKNOWN, 3.1: UNKNOWN

Description

Our nightly CI have been catching this bug since several weeks.

@tenderlovemaking (Aaron Patterson) and @jemmai (Jemma Issroff) are looking into it, but I'm opening an issue anyway to help ensure it is addressed before the final 3.2.0 release.

```
-- Machine register context ------------------------------------------------
 RIP: 0x000055a34a8a586b RBP: 0x0000000000000010 RSP: 0x00007ffc3c91f870
 RAX: 0x0000000000000010 RBX: 0x00007fcf8f671000 RCX: 0xcccccccccccccccd
 RDX: 0x0000000000000010 RDI: 0x00007fcf8f671000 RSI: 0x0000000000000010
  R8: 0x00007fceab611e00  R9: 0x0000000000000060 R10: 0x00007fcf7e94bed5
 R11: 0x0000000000000001 R12: 0x00007fcf8f671000 R13: 0x00007fcd7be526d0
 R14: 0x0000000000000000 R15: 0x00007ffc3c91fc10 EFL: 0x0000000000010246

-- C level backtrace information -------------------------------------------
/usr/local/ruby/bin/ruby(rb_print_backtrace+0x11) [0x55a34aa5d68d] vm_dump.c:770
/usr/local/ruby/bin/ruby(rb_vm_bugreport) vm_dump.c:1065
/usr/local/ruby/bin/ruby(rb_bug_for_fatal_signal+0xee) [0x55a34aafecbe] error.c:819
/usr/local/ruby/bin/ruby(sigsegv+0x4d) [0x55a34a9b315d] signal.c:964
/lib/x86_64-linux-gnu/libpthread.so.0(__restore_rt+0x0) [0x7fcf8feb6420]
/usr/local/ruby/bin/ruby(RVALUE_WB_UNPROTECTED+0x1a) [0x55a34a8a586b] gc.c:1657
/usr/local/ruby/bin/ruby(rgengc_check_relation) gc.c:6918
/usr/local/ruby/bin/ruby(gc_mark_set+0x0) [0x55a34a8a9a52] gc.c:6996
/usr/local/ruby/bin/ruby(gc_mark_ptr) gc.c:6997
/usr/local/ruby/bin/ruby(gc_mark_children+0x5cf) [0x55a34a8aac5f] gc.c:7281
/usr/local/ruby/bin/ruby(gc_mark_stacked_objects+0x2e) [0x55a34a8ac8e6] gc.c:7375
/usr/local/ruby/bin/ruby(gc_mark_stacked_objects_all) gc.c:7415
/usr/local/ruby/bin/ruby(gc_marks_rest) gc.c:8580
/usr/local/ruby/bin/ruby(gc_marks+0x37) [0x55a34a8aeb10] gc.c:8621
/usr/local/ruby/bin/ruby(gc_start) gc.c:9452
/usr/local/ruby/bin/ruby(rb_multi_ractor_p+0x0) [0x55a34a8aeeab] gc.c:9333
/usr/local/ruby/bin/ruby(rb_vm_lock_leave) vm_sync.h:92
/usr/local/ruby/bin/ruby(garbage_collect) gc.c:9335
/usr/local/ruby/bin/ruby(garbage_collect_with_gvl+0x83) [0x55a34a8aef93] gc.c:9715
/usr/local/ruby/bin/ruby(objspace_malloc_increase_body+0x101) [0x55a34a8af0d1] gc.c:12004
/usr/local/ruby/bin/ruby(objspace_malloc_fixup+0x13) [0x55a34a8af387] gc.c:12082
/usr/local/ruby/bin/ruby(objspace_xmalloc0) gc.c:12147
/usr/local/ruby/bin/ruby(RSTRING_LEN+0x0) [0x55a34a9c95b2] string.c:3127
```

We don't know exactly when the bug started because it was hidden by another one in the same path.

History

#1 - 11/04/2022 11:55 PM - jhawthorn (John Hawthorn)

We're also seeing this on GitHub's CI. I spent some time investigating today but didn't yet find the root cause.

For us it always seems to be ROBJECT_IVPTR(obj)[15] which has a bogus value (though that could be a coincidence).

#2 - 11/08/2022 10:18 AM - byroot (Jean Boussier)

I'm no longer seeing this crash, I suspect https://github.com/ruby/ruby/commit/6e4b97f1daf2a6e60dcfb5df4136ce5681095849 fixed it.

@jhawthorn (John Hawthorn) do you confirm?

#3 - 11/08/2022 10:32 PM - jhawthorn (John Hawthorn)

- Status changed from Open to Closed

Yes, I'm seeing the same. Yesterday we bumped from c3de08c to 72c7dba and I haven't seen it since.