

## Ruby master - Bug #16814

### Segmentation fault in GC while running test/ruby/test\_fiber.rb on s390x

04/24/2020 05:31 AM - ReiOdaira (Rei Odaira)

<b>Status:</b>	Assigned	
<b>Priority:</b>	Normal	
<b>Assignee:</b>	ioquatix (Samuel Williams)	
<b>Target version:</b>		
<b>ruby -v:</b>	ruby 2.8.0dev (2020-04-12T03:45:22Z master 5c27681813) [s390x-linux]	<b>Backport:</b> 2.5: DONTNEED, 2.6: DONTNEED, 2.7: REQUIRED

#### Description

A segmentation fault almost always happens in test/ruby/test\_fiber.rb with certain commits of latest Ruby on s390x.

```
$ make test-all TESTS=test/ruby/test_fiber.rb
Run options:
  --seed=90044
  "--ruby=./miniruby -I./lib -I. -I.ext/common ./tool/runruby.rb --extout=.ext -- --disable-gems
"
  --excludes-dir=./test/excludes
  --name=!/memory_leak/

# Running tests:

[24/29] TestFiber#test_stack_size = 0.89 s
  1) Failure:
TestFiber#test_stack_size [/home/chkbuild/my-tmp/build/20200412T043305Z/ruby/test/ruby/test_fiber.
rb:356]:
pid 5713 killed by SIGABRT (signal 6) (core dumped)
| -e:1:in `print': stack level too deep (SystemStackError)
|   from -e:1:in `rec'
|   from -e:1:in `block (3 levels) in rec'
|   from -e:1:in `times'
|   from -e:1:in `block (2 levels) in rec'
|   from -e:1:in `times'
|   from -e:1:in `block in rec'
|   from -e:1:in `times'
|   from -e:1:in `rec'
|   ... 172 levels...
|   from -e:1:in `block in rec'
| -e: [BUG] Segmentation fault at 0x0000000000000000
| ruby 2.8.0dev (2020-04-12T03:45:22Z master 5c27681813) [s390x-linux]
|
| -- Control frame information -----
| c:0001 p:0000 s:0003 E:001e20 (none) [FINISH]
|
| -- Other runtime information -----
|
| * Loaded script: -e
|
| * Loaded features:
|
|   0 enumerator.so
|   1 thread.rb
|   2 rational.so
|   3 complex.so
|   4 ruby2_keywords.rb
|   5 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/.ext/s390x-linux/enc/encdb.so
|   6 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/.ext/s390x-linux/enc/trans/transdb.so
|   7 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/rbconfig.rb
|   8 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/compatibility.rb
|   9 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/defaults.rb
```

```

| 10 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/deprecate.rb
| 11 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/errors.rb
| 12 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/version.rb
| 13 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/requirement.rb
| 14 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/platform.rb
| 15 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/basic_specification.rb
| 16 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/stub_specification.rb
| 17 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/util.rb
| 18 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/text.rb
| 19 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/user_interaction.rb
| 20 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/specification_policy.rb
| 21 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/util/list.rb
| 22 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/specification.rb
| 23 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/exceptions.rb
| 24 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/bundler_version_finder.rb
| 25 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/dependency.rb
| 26 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/core_ext/kernel_gem.rb
| 27 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/.ext/s390x-linux/monitor.so
| 28 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/.ext/common/monitor.rb
| 29 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/core_ext/kernel_require.rb
| 30 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems/core_ext/kernel_warn.rb
| 31 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/rubygems.rb
| 32 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/did_you_mean/version.rb
| 33 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/did_you_mean/core_ext/name_error.rb
| 34 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/did_you_mean/levenshtein.rb
| 35 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/did_you_mean/jaro_winkler.rb
| 36 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/did_you_mean/spell_checker.rb
| 37 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/did_you_mean/spell_checkers/name_err
or_checkers/class_name_checker.rb
| 38 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/did_you_mean/spell_checkers/name_err
or_checkers/variable_name_checker.rb
| 39 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/did_you_mean/spell_checkers/name_err
or_checkers.rb
| 40 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/did_you_mean/spell_checkers/method_n
ame_checker.rb
| 41 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/did_you_mean/spell_checkers/key_err
or_checker.rb
| 42 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/did_you_mean/spell_checkers/null_che
cker.rb
| 43 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/did_you_mean/formatters/plain_format
ter.rb
| 44 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/did_you_mean/tree_spell_checker.rb
| 45 /home/chkbuild/my-tmp/build/20200412T043305Z/ruby/lib/did_you_mean.rb
|
| * Process memory map:
|
| 2aa1538000-2aa15772000 r-xp 00000000 5e:01 1198050 /home/chkbuild/my-tmp/b
uild/20200412T043305Z/ruby/ruby
| 2aa15772000-2aa15777000 r--p 003f1000 5e:01 1198050 /home/chkbuild/my-tmp/b
uild/20200412T043305Z/ruby/ruby
| 2aa15777000-2aa15779000 rw-p 003f6000 5e:01 1198050 /home/chkbuild/my-tmp/b
uild/20200412T043305Z/ruby/ruby
| 2aa15779000-2aa15787000 rw-p 00000000 00:00 0
| 2aa29766000-2aa29ab0000 rw-p 00000000 00:00 0 [heap]
| 3ffaa180000-3ffaa182000 r-xp 00000000 5e:01 1197862 /home/chkbuild/my-tmp/b
uild/20200412T043305Z/ruby/.ext/s390x-linux/monitor.so
| 3ffaa182000-3ffaa183000 r--p 00001000 5e:01 1197862 /home/chkbuild/my-tmp/b
uild/20200412T043305Z/ruby/.ext/s390x-linux/monitor.so
| 3ffaa183000-3ffaa184000 rw-p 00002000 5e:01 1197862 /home/chkbuild/my-tmp/b
uild/20200412T043305Z/ruby/.ext/s390x-linux/monitor.so
| 3ffaa200000-3ffaa202000 r-xp 00000000 5e:01 1198135 /home/chkbuild/my-tmp/b
uild/20200412T043305Z/ruby/.ext/s390x-linux/enc/trans/transdb.so
| 3ffaa202000-3ffaa203000 ---p 00002000 5e:01 1198135 /home/chkbuild/my-tmp/b
uild/20200412T043305Z/ruby/.ext/s390x-linux/enc/trans/transdb.so
| 3ffaa203000-3ffaa204000 r--p 00002000 5e:01 1198135 /home/chkbuild/my-tmp/b
uild/20200412T043305Z/ruby/.ext/s390x-linux/enc/trans/transdb.so
| 3ffaa204000-3ffaa205000 rw-p 00003000 5e:01 1198135 /home/chkbuild/my-tmp/b

```

```

uild/20200412T043305Z/ruby/.ext/s390x-linux/enc/trans/transdb.so
| 3ffaab76000-3ffacc80000 rw-p 00000000 00:00 0
| 3ffacc80000-3ffacc82000 r-xp 00000000 5e:01 133388 /usr/lib64/libfreebl3.s
o
| 3ffacc82000-3ffacc83000 r--p 00001000 5e:01 133388 /usr/lib64/libfreebl3.s
o
| 3ffacc83000-3ffacc84000 rw-p 00002000 5e:01 133388 /usr/lib64/libfreebl3.s
o
| 3ffacd00000-3ffaceaf000 r-xp 00000000 5e:01 134626 /usr/lib64/libc-2.17.so
| 3ffaceaf000-3ffaceb3000 r--p 001ae000 5e:01 134626 /usr/lib64/libc-2.17.so
| 3ffaceb3000-3ffaceb5000 rw-p 001b2000 5e:01 134626 /usr/lib64/libc-2.17.so
| 3ffaceb5000-3ffaceb9000 rw-p 00000000 00:00 0
| 3ffacf00000-3ffacfa8000 r-xp 00000000 5e:01 135803 /usr/lib64/libm-2.17.so
| 3ffacfa8000-3ffacfa9000 r--p 000a7000 5e:01 135803 /usr/lib64/libm-2.17.so
| 3ffacfa9000-3ffacfaa000 rw-p 000a8000 5e:01 135803 /usr/lib64/libm-2.17.so
| 3ffad000000-3ffad00d000 r-xp 00000000 5e:01 135760 /usr/lib64/libcrypt-2.1
7.so
| 3ffad00d000-3ffad00e000 r--p 0000c000 5e:01 135760 /usr/lib64/libcrypt-2.1
7.so
| 3ffad00e000-3ffad00f000 rw-p 0000d000 5e:01 135760 /usr/lib64/libcrypt-2.1
7.so
| 3ffad00f000-3ffad03d000 rw-p 00000000 00:00 0
| 3ffad080000-3ffad083000 r-xp 00000000 5e:01 135797 /usr/lib64/libdl-2.17.s
o
| 3ffad083000-3ffad084000 r--p 00002000 5e:01 135797 /usr/lib64/libdl-2.17.s
o
| 3ffad084000-3ffad085000 rw-p 00003000 5e:01 135797 /usr/lib64/libdl-2.17.s
o
| 3ffad100000-3ffad187000 r-xp 00000000 5e:01 136942 /usr/lib64/libgmp.so.10
.2.0
| 3ffad187000-3ffad189000 r--p 00086000 5e:01 136942 /usr/lib64/libgmp.so.10
.2.0
| 3ffad189000-3ffad18a000 rw-p 00088000 5e:01 136942 /usr/lib64/libgmp.so.10
.2.0
| 3ffad200000-3ffad208000 r-xp 00000000 5e:01 136149 /usr/lib64/librt-2.17.s
o
| 3ffad208000-3ffad209000 r--p 00007000 5e:01 136149 /usr/lib64/librt-2.17.s
o
| 3ffad209000-3ffad20a000 rw-p 00008000 5e:01 136149 /usr/lib64/librt-2.17.s
o
| 3ffad280000-3ffad298000 r-xp 00000000 5e:01 135793 /usr/lib64/libpthread-2
.17.so
| 3ffad298000-3ffad299000 r--p 00017000 5e:01 135793 /usr/lib64/libpthread-2
.17.so
| 3ffad299000-3ffad29a000 rw-p 00018000 5e:01 135793 /usr/lib64/libpthread-2
.17.so
| 3ffad29a000-3ffad29e000 rw-p 00000000 00:00 0
| 3ffad300000-3ffad317000 r-xp 00000000 5e:01 136264 /usr/lib64/libz.so.1.2.
7
| 3ffad317000-3ffad318000 r--p 00016000 5e:01 136264 /usr/lib64/libz.so.1.2.
7
| 3ffad318000-3ffad319000 rw-p 00017000 5e:01 136264 /usr/lib64/libz.so.1.2.
7
| 3ffad380000-3ffad382000 r-xp 00000000 5e:01 1198055 /home/chkbuild/my-tmp/b
uild/20200412T043305Z/ruby/.ext/s390x-linux/enc/encdb.so
| 3ffad382000-3ffad383000 r--p 00001000 5e:01 1198055 /home/chkbuild/my-tmp/b
uild/20200412T043305Z/ruby/.ext/s390x-linux/enc/encdb.so
| 3ffad383000-3ffad384000 rw-p 00002000 5e:01 1198055 /home/chkbuild/my-tmp/b
uild/20200412T043305Z/ruby/.ext/s390x-linux/enc/encdb.so
| 3ffad39f000-3ffad400000 rw-p 00000000 00:00 0
| 3ffad400000-3ffad423000 r-xp 00000000 5e:01 133698 /usr/lib64/ld-2.17.so
| 3ffad424000-3ffad425000 r--p 00023000 5e:01 133698 /usr/lib64/ld-2.17.so
| 3ffad425000-3ffad426000 rw-p 00024000 5e:01 133698 /usr/lib64/ld-2.17.so
| 3ffad426000-3ffad427000 rw-p 00000000 00:00 0
| 3ffad473000-3ffad47e000 rw-p 00000000 00:00 0
| 3ffad47e000-3ffad480000 r-xp 00000000 00:00 0 [vdso]
| 3ffadb181000-3ffadb980000 rw-p 00000000 00:00 0 [stack]

```

```
|
|
Finished tests in 7.935617s, 3.6544 tests/s, 23.9427 assertions/s.
29 tests, 190 assertions, 1 failures, 0 errors, 0 skips
```

```
ruby -v: ruby 2.8.0dev (2020-04-12T03:45:22Z master 5c27681813) [s390x-linux]
make: *** [yes-test-all] Error 1
```

The segmentation fault happens in a Ruby script invoked from `test_fiber.rb` by `EnvUtil.invoke_ruby()`. The Ruby script is to deliberately cause a stack overflow as follows.

```
$stdout.sync=true; def rec; print "."; 1.times{1.times{1.times{rec}}}; end; Fiber.new{rec}.resume
```

On s390x, this script caused `SystemStackError`, which I think is expected. However, it was during the handling of the stack overflow when the segmentation fault happened.

The core dump shows the following stack trace.

```
(gdb) bt
#0 0x000003fffb62c1350 in raise () from /lib64/libc.so.6
#1 0x000003fffb62c2bd8 in abort () from /lib64/libc.so.6
#2 0x000002aa0c84bf9a in die () at error.c:646
#3 rb_bug_for_fatal_signal (default_sighandler=0x0, sig=sig@entry=11,
    ctx=ctx@entry=0x2aa2d18fc50,
    fmt=fmt@entry=0x2aa0c89352c "Segmentation fault at %p") at error.c:678
#4 0x000002aa0c6fbd60 in sigsegv (sig=<optimized out>, info=0x2aa2d18fbd0,
    ctx=0x2aa2d18fc50) at signal.c:955
#5 <signal handler called>
#6 0x000002aa0c5dlf36 in gc_mark_children (
    objspace=objspace@entry=0x2aa2d09c6b0, obj=obj@entry=2929923415200)
    at gc.c:5478
#7 0x000002aa0c5d3ac8 in rgen_gc_rememberset_mark (heap=0x2aa2d09c6d8,
    objspace=0x2aa2d09c6b0) at gc.c:6747
#8 gc_marks_start (full_mark=<optimized out>, objspace=0x2aa2d09c6b0)
    at gc.c:6314
#9 gc_marks (full_mark=<optimized out>, objspace=0x2aa2d09c6b0) at gc.c:6583
#10 gc_start (objspace=objspace@entry=0x2aa2d09c6b0, reason=<optimized out>,
    reason@entry=256) at gc.c:7370
#11 0x000002aa0c5a9370 in heap_prepare (heap=0x2aa2d09c6d8,
    objspace=<optimized out>) at gc.c:1977
#12 heap_get_freeobj_from_next_freepage (
    objspace=objspace@entry=0x2aa2d09c6b0, heap=heap@entry=0x2aa2d09c6d8)
    at gc.c:1989
---Type <return> to continue, or q <return> to quit---
#13 0x000002aa0c5d7cb0 in heap_get_freeobj (heap=0x2aa2d09c6d8,
    objspace=0x2aa2d09c6b0) at gc.c:2028
#14 newobj_slowpath (wb_protected=1, objspace=0x2aa2d09c6b0, v3=v3@entry=0,
    v2=0, v1=0, flags=5, klass=2929923683840) at gc.c:2170
#15 newobj_slowpath_wb_protected (klass=2929923683840, flags=5, v1=v1@entry=0,
    v2=v2@entry=0, v3=v3@entry=0, objspace=0x2aa2d09c6b0) at gc.c:2182
#16 0x000002aa0c5d817c in newobj_of (wb_protected=1, v3=0, v2=0, v1=0,
    flags=5, klass=<optimized out>) at gc.c:2218
#17 rb_wb_protected_newobj_of (klass=<optimized out>, flags=flags@entry=5)
    at gc.c:2234
#18 0x000002aa0c710fa2 in str_alloc (klass=<optimized out>) at string.c:745
#19 str_new0 (klass=<optimized out>, ptr=0x2aa0c85ad0e "\t", len=1,
    termolen=<optimized out>) at string.c:767
#20 0x000002aa0c5b1f28 in ruby3_str_new_cstr (str=0x2aa0c85ad0e "\t")
    at ./include/ruby/3/intern/string.h:159
#21 print_backtrace (eclass=2929923530680, errat=errat@entry=2929923354920,
    str=str@entry=8, reverse=reverse@entry=0) at eval_error.c:250
#22 0x000002aa0c5b3f68 in print_backtrace (reverse=0, str=8,
    errat=<optimized out>, eclass=<optimized out>) at eval_error.c:233
#23 rb_error_write (reverse=0, highlight=0, str=8, errat=<optimized out>,
    emesg=2929923530600, errinfo=<optimized out>) at eval_error.c:340
```

```
#24 rb_ec_error_print (ec=ec@entry=0x2aa2d09cb40, errinfo=<optimized out>)
    at eval_error.c:365
#25 0x000002aa0c5b4572 in error_handle (ec=0x2aa2d09cb40, ex=<optimized out>)
---Type <return> to continue, or q <return> to quit---
    at eval_error.c:478
#26 0x000002aa0c5b4d50 in rb_ec_cleanup (ec=ec@entry=0x2aa2d09cb40,
    ex=<optimized out>) at eval.c:241
#27 0x000002aa0c5b565a in ruby_run_node (n=0x2aa2d0b6128) at eval.c:348
#28 0x000002aa0c5af68a in main (argc=3, argv=0x3ffd127e9e8) at ./main.c:50
```

At gc.c:5478, the segmentation fault happened because any->as.typeddata.type was 0. as.typeddata.type should not be 0 for RTypedData.

```
5473         case T_DATA:
5474             {
5475                 void *const ptr = DATA_PTR(obj);
5476                 if (ptr) {
5477                     RUBY_DATA_FUNC mark_func = RTYPEDDATA_P(obj) ?
5478                         any->as.typeddata.type->function.dmark :
5479                         any->as.data.dmark;
5480                     if (mark_func) (*mark_func)(ptr);
5481                 }
5482             }
5483             break;
```

This is a timing bug, but it almost always happens with 5c27681813. It is not clear to which commit this issue is related. In Ruby CI, it started happening in early February 2020 and stopped showing up after increasing the stack size by ulimit -s. It started happening again in early April 2020 and disappeared on April 15.

Anybody has any ideas how I should debug this?

## History

### #1 - 04/24/2020 06:07 AM - nobu (Nobuyoshi Nakada)

Where does any->as.data.free point?

Is any->as.basic.klass a valid class object?

If you compile gc.c as make DEFS=-DGC\_DEBUG gc.o, any->file and any->line have the location in ruby level, and could help you.

### #2 - 04/24/2020 06:38 AM - mame (Yusuke Endoh)

disappeared on April 15.

You may know, but the test has been skipped on s390x since 9948adda67f4b7a6e3575f1eba9025f998811d2.

### #3 - 04/24/2020 11:05 PM - ReiOdaire (Rei Odaire)

Did you mean any->as.data.dfree? It points to no valid location.

```
(gdb) print any->as.data
$4 = {basic = {flags = 12, klass = 2930849422520}, dmark = 0x0, dfree = 0x1,
    data = 0x2aa6449f9e0}
(gdb) print any->as.typeddata
$5 = {basic = {flags = 12, klass = 2930849422520}, type = 0x0, typed_flag = 1,
    data = 0x2aa6449f9e0}
```

any->as.basic.klass seems to be a valid class. Is there any way to figure out what class it is using the core dump file?

```
(gdb) print *(struct RBasic *)any->as.basic.klass
$7 = {flags = 98, klass = 2930849422480}
(gdb) print ((struct RBasic *)any->as.basic.klass)->flags & 0x1f
$9 = 2
```

I've tried make DEFS=-DGC\_DEBUG gc.o. It made the test fail quite less often than before, and when it failed, it did at a different location in GC (gc.c:5240), but it will help a lot. Thanks.

Thanks, Endoh-san, I didn't know the test was skipped.

#### #4 - 04/26/2020 05:13 PM - mame (Yusuke Endoh)

FYI: I re-enabled the test in question with 93ed465dcdc866013cd93c3662937497900c8086

#### #5 - 05/14/2020 10:50 AM - ioquatix (Samuel Williams)

[mame \(Yusuke Endoh\)](#) I have merged the light weight concurrency patch, and it included some changes to these tests to make them less flaky, by putting it in separate test file. In my experience it seems much more reliable now. Just FYI.

#### #6 - 05/25/2020 02:08 AM - ioquatix (Samuel Williams)

Can you check if this is still a problem, I merged my changes which should make this test more reliable. But I did not fix any underlying problems.

#### #7 - 05/31/2020 07:42 AM - ReiOdaira (Rei Odaira)

On s390x, FIBER\_POOL\_ALLOCATION\_FREE is enabled. The doubly linked list of fiber\_pool->vacancies assumes that the head fiber\_pool\_vacancy has NULL in its previous field. However, when a fiber is released, fiber\_pool\_vacancy\_push() called from fiber\_pool\_stack\_release() does not store NULL to vacancy->previous.

Why this caused the observed symptom:

As test\_stack\_size uses up the VM stack of the fiber, it writes something into the memory location where struct fiber\_pool\_vacancy would reside if the stack were free. When the fiber is released, the stack's fiber\_pool\_vacancy is returned to the head of the vacancies doubly linked list, and then fiber\_pool\_allocation\_free() is triggered. fiber\_pool\_vacancy\_remove() manipulates the doubly linked list, and the vacancy->previous of the released fiber should have been NULL because it is at the head of the list.

```
if (vacancy->previous) {
    vacancy->previous->next = vacancy->next;
}
```

However, since vacancy->previous contains arbitrary data, the code snippet above destroys the memory location that happens to be pointed to by vacancy->previous. In test\_stack\_size, vacancy->previous happens to point to an encoding object that is live, and vacancy->next happens to be 0. This means vacancy->previous->next = vacancy->next; writes 0 into the as.typeddata.type field of the live object. This finally leads to the segmentation fault during GC.

#### #8 - 05/31/2020 08:21 AM - ioquatix (Samuel Williams)

[ReiOdaira \(Rei Odaira\)](#) thanks for your careful analysis. It is very useful! I will review the code and get back to you.

#### #9 - 06/04/2020 10:05 AM - ioquatix (Samuel Williams)

```
inline static struct fiber_pool_vacancy *
fiber_pool_vacancy_push(struct fiber_pool_vacancy * vacancy, struct fiber_pool_vacancy * head)
{
    vacancy->next = head;

#ifdef FIBER_POOL_ALLOCATION_FREE
    if (head) {
        head->previous = vacancy;
        vacancy->previous = NULL; // added
    }
#endif

    return vacancy;
}
```

[ReiOdaira \(Rei Odaira\)](#) do you think that's sufficient?

#### #10 - 06/04/2020 10:38 AM - ioquatix (Samuel Williams)

<https://github.com/ruby/ruby/pull/3182>

#### #11 - 06/04/2020 11:11 AM - ioquatix (Samuel Williams)

By the way, I've also removed all skips when I rewrote tests into test/ruby/test\_stack.rb.

#### #12 - 06/04/2020 11:42 PM - ioquatix (Samuel Williams)

- Assignee set to ioquatix (Samuel Williams)

- Status changed from Open to Assigned

I have merged this.

[ReiOdaira \(Rei Odaira\)](#) thanks for your effort, you deserve all the credit for tracking down this issue.

Can you please confirm whether the original issue is fixed? If so, we can close this issue.

Thanks!

**#13 - 06/06/2020 02:23 AM - nagachika (Tomoyuki Chikanaga)**

- Backport changed from 2.5: UNKNOWN, 2.6: UNKNOWN, 2.7: UNKNOWN to 2.5: DONTNEED, 2.6: DONTNEED, 2.7: REQUIRED