

Ruby - Bug #20155

Using value of rb_fiber_scheduler_current() crashes Ruby

01/05/2024 10:14 PM - paddor (Patrik Wenger)

Status:	Assigned	
Priority:	Normal	
Assignee:	ioquatix (Samuel Williams)	
Target version:		
ruby -v:	ruby 3.3.0 (2023-12-25 revision 5124f9ac75) [x86_64-linux]	Backport: 3.0: UNKNOWN, 3.1: UNKNOWN, 3.2: UNKNOWN, 3.3: UNKNOWN

Description

While trying to manually block/unblock fibers from an extension using the Fiber Scheduler, I noticed that using the return value of rb_fiber_scheduler_current() crashes Ruby.

I've created a minimal extension gem called "fiber_blocker". Its test suite shows the behavior. See https://github.com/paddor/fiber_blocker, especially the lines containing FIXME.

Passing Fiber.scheduler to the extension functions works. But letting it get the current scheduler itself does not seem to work.

Is rb_fiber_scheduler_current()(within a non-blocking Fiber) not the equivalent to Fiber.scheduler? Even just printing the its return value with #p will crash Ruby.

Ruby either crashes like this:

```
# Running:

T1 BEGIN
T2 BEGIN
T1 END
..T1 BEGIN
ext: blocking fiber
passed scheduler = #<Scheduler:0x00007fc5f22d39e8 @readable={}, @writable={}, @waiting={}, @closed=false, @lock=#<Thread::Mutex:0x00007fc5f22ec8d0>, @blocking={}, @ready=[], @urgent=[#<IO:fd 5>, #<IO:fd 6>]>
T2 BEGIN
ext: unblocking fiber
T1 END
.E

Finished in 1.007014s, 3.9721 runs/s, 2.9791 assertions/s.

1) Error:
TestFiberBlocker#test_fiber_blocker_current_fiber:
fatal: machine stack overflow in critical region
No backtrace
```

Or with a segfault:

```
# Running:

FiberBlocker.test works.
.T1 BEGIN
T2 BEGIN
T1 END
.T1 BEGIN
ext: blocking fiber
/home/user/dev/oss/async_ruby_test/rbnng/fiber_blocker/test/test_fiber_blocker.rb:40: [BUG] Segmentation fault at 0x00000000390d8f98
ruby 3.3.0 (2023-12-25 revision 5124f9ac75) [x86_64-linux]

-- Control frame information -----
c:0003 p:---- s:0012 e:000011 CFUNC :block_fiber
```

```

c:0002 p:0014 s:0006 e:000005 BLOCK  /home/user/dev/oss/async_ruby_test/rbnng/fiber_blocker/test/t
est_fiber_blocker.rb:40 [FINISH]
c:0001 p:---- s:0003 e:000002 DUMMY  [FINISH]

-- Ruby level backtrace information -----
/home/user/dev/oss/async_ruby_test/rbnng/fiber_blocker/test/test_fiber_blocker.rb:40:in `block in
test_fiber_blocking_in_ext'
/home/user/dev/oss/async_ruby_test/rbnng/fiber_blocker/test/test_fiber_blocker.rb:40:in `block_fib
er'

-- Threading information -----
Total ractor count: 1
Ruby thread count for this ractor: 4

-- Machine register context -----
RIP: 0x00007f1554f17ad8 RBP: 0x00000000390d8f90 RSP: 0x00007f153a79e280
RAX: 0x00007f1554addba8 RBX: 0x00007f153a79eab0 RCX: 0x0000000000000000
RDX: 0x00007f1554ade600 RDI: 0x00007f15551e8788 RSI: 0x00000000000000ae1
R8: 0x0000000000000002b R9: 0x00007f153a79f038 R10: 0x00007f1554c0b9b0
R11: 0x00007f153a79e490 R12: 0x00000000000000ae1 R13: 0x0000000000000000
R14: 0x0000000000000000 R15: 0x000055ab732d7df0 EFL: 0x0000000000010206

-- C level backtrace information -----
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_print_backtrace+0x14) [0x7f1554f24961] /home/u
ser/src/ruby-3.3.0/vm_dump.c:820
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_vm_bugreport) /home/user/src/ruby-3.3.0/vm_dum
p.c:1151
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_bug_for_fatal_signal+0x104) [0x7f1554d1c214] /
home/user/src/ruby-3.3.0/error.c:1065
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(sigsegv+0x4f) [0x7f1554e700df] /home/user/src/rub
y-3.3.0/signal.c:926
/lib/x86_64-linux-gnu/libc.so.6(0x7f1554842520) [0x7f1554842520]
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(RBASIC_CLASS+0x0) [0x7f1554f17ad8] ./include/ruby
/internal/globals.h:178
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(gccct_method_search) /home/user/src/ruby-3.3.0/vm
_eval.c:475
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_funcallv_scope) /home/user/src/ruby-3.3.0/vm_e
val.c:1063
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_funcallv) /home/user/src/ruby-3.3.0/vm_eval.c:
1084
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_inspect+0x19) [0x7f1554dc1569] /home/user/src/
ruby-3.3.0/object.c:697
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(ruby__sfvextra+0x11a) [0x7f1554e7223a] /home/user
/src/ruby-3.3.0/sprintf.c:1119
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(BSD_vfprintf+0xa69) [0x7f1554e73059] /home/user/s
rc/ruby-3.3.0/vsnprintf.c:830
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(RBASIC_SET_CLASS_RAW+0x0) [0x7f1554e75b56] /home/
user/src/ruby-3.3.0/sprintf.c:1168
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(ruby_vsprintf0) /home/user/src/ruby-3.3.0/sprintf
.c:1169
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_enc_vsprintf+0x5d) [0x7f1554e75ecd] /home/user
/src/ruby-3.3.0/sprintf.c:1195
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_sprintf+0x9d) [0x7f1554e7607d] /home/user/src/
ruby-3.3.0/sprintf.c:1225
/home/user/dev/oss/async_ruby_test/rbnng/fiber_blocker/lib/fiber_blocker/fiber_blocker.so(block_fi
ber+0x4a) [0x7f1554ad430a] ../../../../ext/fiber_blocker/fiber_blocker.c:29
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(vm_cfp_consistent_p+0x0) [0x7f1554ef64b4] /home/u
ser/src/ruby-3.3.0/vm_insnhelper.c:3490
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(vm_call_cfunc_with_frame_) /home/user/src/ruby-3.
3.0/vm_insnhelper.c:3492
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(vm_call_cfunc_with_frame) /home/user/src/ruby-3.3
.0/vm_insnhelper.c:3518
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(vm_call_cfunc_other) /home/user/src/ruby-3.3.0/vm
_insnhelper.c:3544
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(vm_sendish+0x9e) [0x7f1554f06f87] /home/user/src/
ruby-3.3.0/vm_insnhelper.c:5581
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(vm_exec_core) /home/user/src/ruby-3.3.0/insns.def

```

```
:834
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_vm_exec+0x19a) [0x7f1554f0d1fa] /home/user/src
/ruby-3.3.0/vm.c:2486
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_vm_invoke_proc+0x5f) [0x7f1554f12e0f] /home/us
er/src/ruby-3.3.0/vm.c:1728
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_fiber_start+0x1ba) [0x7f1554cf098a] /home/user
/src/ruby-3.3.0/cont.c:2536
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(fiber_entry+0x20) [0x7f1554cf0d00] /home/user/src
/ruby-3.3.0/cont.c:847
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_threadptr_root_fiber_setup) (null):0
```

This happens with the Async scheduler as well as with Ruby's test scheduler. My minimal extension uses Ruby's.

I hope I'm not missing something obvious. My C isn't very good.

History

#1 - 01/06/2024 03:41 PM - paddor (Patrik Wenger)

- Description updated

#2 - 01/16/2024 08:46 PM - paddor (Patrik Wenger)

[@ioquatix \(Samuel Williams\)](#) Could you have a look at this? I have a feeling I'm missing something obvious.

#3 - 01/16/2024 09:00 PM - ioquatix (Samuel Williams)

- Status changed from Open to Assigned

- Assignee set to ioquatix (Samuel Williams)

Thanks for the report, I'll need to investigate.

#4 - 01/16/2024 09:17 PM - ioquatix (Samuel Williams)

Can you tell me the exact commit/revision which was running:

```
/home/user/dev/oss/async_ruby_test/rbnnng/fiber_blocker/lib/fiber_blocker/fiber_blocker.so(block_fiber+0x4a) [0
x7f1554ad430a] ../../../../../../ext/fiber_blocker/fiber_blocker.c:29
```

#5 - 01/16/2024 09:27 PM - ioquatix (Samuel Williams)

Here is the implementation from CRuby:

```
static VALUE
rb_fiber_scheduler_current_for_threadptr(rb_thread_t *thread)
{
    VM_ASSERT(thread);

    if (thread->blocking == 0) {
        return thread->scheduler;
    }
    else {
        return Qnil;
    }
}

VALUE
rb_fiber_scheduler_current(void)
{
    return rb_fiber_scheduler_current_for_threadptr(GET_THREAD());
}
```

As you can see, it's not particularly complex.

Maybe the problem is trying to print it out. I'm actually not sure if you can write `p Fiber.scheduler` - I mean, in theory it should work.

#6 - 01/16/2024 11:01 PM - paddor (Patrik Wenger)

Thanks for looking into this. I'm pretty sure it was that one (initial) commit in the `fiber_blocker` repo. My extension (a PR for the `rbnnng` gem [1]) would ideally block/unblock fibers using NNG's `nng_aio_*`() functions [2]. That's how I noticed the crashes. Trying to print the `Fiber.scheduler` came afterwards.

[1] <https://github.com/adibsaad/rbnnng>

[2] https://nng.nanomsg.org/man/tip/nng_aio.5.html

#7 - 01/16/2024 11:16 PM - ioquatix (Samuel Williams)

Line 29 does not point to any meaningful statement: https://github.com/paddor/fiber_blocker/blob/main/ext/fiber_blocker/fiber_blocker.c#L29 - can you check it?

#8 - 01/17/2024 12:32 AM - paddor (Patrik Wenger)

You're right. It was line 28, the one with `rb_fiber_scheduler_block(scheduler, blocker, timeout)`.

I just ran it again with the commit I just pushed (which enables the bad line in the test `#test_fiber_blocking_in_ext` on line 44):

```
$ bundle exec rake compile; and bundle exec rake test

[625/2578]
/usr/bin/gmake install sitearchdir=../../../../../lib/fiber_blocker sitelibdir=../../../../../lib/fiber_blocker targ
et_prefix=
/usr/bin/install -c -m 0755 fiber_blocker.so ../../../../../lib/fiber_blocker
cp tmp/x86_64-linux/fiber_blocker/3.3.0/fiber_blocker.so tmp/x86_64-linux/stage/lib/fiber_blocker/fiber_blocke
r.so
/home/user/.rubies/ruby-3.3.0/lib/ruby/gems/3.3.0/gems/minitest-5.20.0/lib/minitest.rb:3: warning: mutex_m was
loaded from the standard library, but will no longer be part of the default gems since Ruby 3.4.0. Add mutex_
m to your Gemfile or gems
pec. Also contact author of minitest-5.20.0 to add mutex_m into its gemspec.
/home/user/dev/oss/async_ruby_test/rbnng/fiber_blocker/test/test_fiber_blocker.rb:23: warning: assigned but un
used variable - f2
/home/user/dev/oss/async_ruby_test/rbnng/fiber_blocker/test/test_fiber_blocker.rb:50: warning: assigned but un
used variable - f2
Run options: --seed 61169

# Running:

T1 BEGIN
ext: blocking fiber
/home/user/dev/oss/async_ruby_test/rbnng/fiber_blocker/test/test_fiber_blocker.rb:44: [BUG] Segmentation fault
at 0x00000000760f53c8
ruby 3.3.0 (2023-12-25 revision 5124f9ac75) [x86_64-linux]

-- Control frame information -----
c:0003 p:---- s:0012 e:000011 CFUNC :block_fiber
c:0002 p:0014 s:0006 e:000005 BLOCK /home/user/dev/oss/async_ruby_test/rbnng/fiber_blocker/test/test_fiber_b
l
ocker.rb:44 [FINISH]
c:0001 p:---- s:0003 e:000002 DUMMY [FINISH]

-- Ruby level backtrace information -----
/home/user/dev/oss/async_ruby_test/rbnng/fiber_blocker/test/test_fiber_blocker.rb:44:in `block in test_fiber_b
locking_in_ext'
/home/user/dev/oss/async_ruby_test/rbnng/fiber_blocker/test/test_fiber_blocker.rb:44:in `block_fiber'

-- Threading information -----
Total ractor count: 1
Ruby thread count for this ractor: 4

-- Machine register context -----
RIP: 0x00007faf91f17ad8 RBP: 0x00000000760f53c0 RSP: 0x00007faf777deb40
RAX: 0x00007faf9227eba8 RBX: 0x0000556e56e3f170 RCX: 0x00007faf777dec30
RDX: 0x00007faf9227f600 RDI: 0x00007faf921e8788 RSI: 0x000000000000067e1
R8: 0x0000000000000000 R9: 0x00007faf777df038 R10: 0x00007faf91c05a40
R11: 0x00007faf91e6d060 R12: 0x000000000000067e1 R13: 0x00007faf777dec30
R14: 0x0000000000000002 R15: 0x0000556e56c17ff0 EFL: 0x00000000000010206

-- C level backtrace information -----
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_print_backtrace+0x14) [0x7faf91f24961] /home/user/src/ruby
-3.3.0/vm_dump.c:820
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_vm_bugreport) /home/user/src/ruby-3.3.0/vm_dump.c:1151
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_bug_for_fatal_signal+0x104) [0x7faf91d1c214] /home/user/sr
c/ruby-3.3.0/error.c:1065
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(sigsegv+0x4f) [0x7faf91e700df] /home/user/src/ruby-3.3.0/sign
al.c:926
/lib/x86_64-linux-gnu/libc.so.6(0x7faf91842520) [0x7faf91842520]
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(RBASIC_CLASS+0x0) [0x7faf91f17ad8] ./include/ruby/internal/gl
obals.h:178
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(gccct_method_search) /home/user/src/ruby-3.3.0/vm_eval.c:475
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_funcallv_scope) /home/user/src/ruby-3.3.0/vm_eval.c:1063
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_funcallv) /home/user/src/ruby-3.3.0/vm_eval.c:1084
```

```

/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_fiber_scheduler_block+0x3e) [0x7faf91e6d09e] /home/user/src/ruby-3.3.0/scheduler.c:369
/home/user/dev/oss/async_ruby_test/rbnnng/fiber_blocker/lib/fiber_blocker/fiber_blocker.so(block_fiber+0x3e) [0x7faf922043be] ../../../../ext/fiber_blocker/fiber_blocker.c:28
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(vm_cfp_consistent_p+0x0) [0x7faf91ef64b4] /home/user/src/ruby-3.3.0/vm_insnhelper.c:3490
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(vm_call_cfunc_with_frame_) /home/user/src/ruby-3.3.0/vm_insnhelper.c:3492
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(vm_call_cfunc_with_frame) /home/user/src/ruby-3.3.0/vm_insnhelper.c:3518
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(vm_call_cfunc_other) /home/user/src/ruby-3.3.0/vm_insnhelper.c:3544
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(vm_sendish+0x9e) [0x7faf91f06f87] /home/user/src/ruby-3.3.0/vm_insnhelper.c:5581
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(vm_exec_core) /home/user/src/ruby-3.3.0/insns.def:834
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_vm_exec+0x19a) [0x7faf91f0d1fa] /home/user/src/ruby-3.3.0/vm.c:2486
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_vm_invoke_proc+0x5f) [0x7faf91f12e0f] /home/user/src/ruby-3.3.0/vm.c:1728
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_fiber_start+0x1ba) [0x7faf91cf098a] /home/user/src/ruby-3.3.0/cont.c:2536
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(fiber_entry+0x20) [0x7faf91cf0d00] /home/user/src/ruby-3.3.0/cont.c:847
/home/user/.rubies/ruby-3.3.0/lib/libruby.so.3.3(rb_threadptr_root_fiber_setup) (null):0

```

#9 - 01/17/2024 01:42 AM - ioquatix (Samuel Williams)

Here is an example of valid usage:

```

static VALUE
call_rb_fiber_scheduler_block(VALUE mutex)
{
    return rb_fiber_scheduler_block(rb_fiber_scheduler_current(), mutex, Qnil);
}

```

taken from thread_sync.c.

When I tried to compile your code, I got a lot of errors:

```

../../../../ext/fiber_blocker/fiber_blocker.c:15:21: error: call to undeclared function 'rb_fiber_scheduler_current'; ISO C99 and later do not support implicit function declarations [-Wimplicit-function-declaration]
    VALUE scheduler = rb_fiber_scheduler_current();
                        ^
../../../../ext/fiber_blocker/fiber_blocker.c:24:21: error: call to undeclared function 'rb_fiber_scheduler_current'; ISO C99 and later do not support implicit function declarations [-Wimplicit-function-declaration]
    VALUE scheduler = rb_fiber_scheduler_current();
                        ^
../../../../ext/fiber_blocker/fiber_blocker.c:28:14: error: call to undeclared function 'rb_fiber_scheduler_block'; ISO C99 and later do not support implicit function declarations [-Wimplicit-function-declaration]
    result = rb_fiber_scheduler_block(scheduler, blocker, timeout);
              ^
../../../../ext/fiber_blocker/fiber_blocker.c:40:22: error: call to undeclared function 'rb_fiber_scheduler_current'; ISO C99 and later do not support implicit function declarations [-Wimplicit-function-declaration]
    VALUE scheduler2 = rb_fiber_scheduler_current();
                        ^
../../../../ext/fiber_blocker/fiber_blocker.c:47:14: error: call to undeclared function 'rb_fiber_scheduler_block'; ISO C99 and later do not support implicit function declarations [-Wimplicit-function-declaration]
    result = rb_fiber_scheduler_block(scheduler, blocker, timeout);
              ^
../../../../ext/fiber_blocker/fiber_blocker.c:40:9: warning: unused variable 'scheduler2' [-Wunused-variable]
    VALUE scheduler2 = rb_fiber_scheduler_current();
    ^
../../../../ext/fiber_blocker/fiber_blocker.c:59:18: error: call to undeclared function 'rb_fiber_scheduler_unblock'; ISO C99 and later do not support implicit function declarations [-Wimplicit-function-declaration]
    VALUE result = rb_fiber_scheduler_unblock(scheduler, blocker, fiber);
                  ^
../../../../ext/fiber_blocker/fiber_blocker.c:67:3: warning: incompatible function pointer types passing 'VALUE (void)' (aka 'unsigned long (void)') to parameter of type 'VALUE (*) (VALUE)' (aka 'unsigned long (*) (unsigned long)') [-Wincompatible-function-pointer-types]
    rb_define_singleton_method(rb_mFiberBlocker, "hello", hello, 0);
    ^~~~~~
/Users/samuel/.rubies/ruby-3.3.0/include/ruby-3.3.0/ruby/internal/anyargs.h:308:143: note: expanded from macro 'rb_define_singleton_method'
#define rb_define_singleton_method(obj, mid, func, arity) RBIMPL_ANYARGS_DISPATCH rb_define_singleton_method((arity), (func))((obj), (mid), (func), (arity))

```

```

^~~~~~
/Users/samuel/.rubies/ruby-3.3.0/include/ruby-3.3.0/ruby/internal/anyargs.h:271:1: note: passing argument to parameter here
RBIMPL_ANYARGS_DECL(rb_define_singleton_method, VALUE, const char *)
^
/Users/samuel/.rubies/ruby-3.3.0/include/ruby-3.3.0/ruby/internal/anyargs.h:255:72: note: expanded from macro 'RBIMPL_ANYARGS_DECL'
RBIMPL_ANYARGS_ATTRSET(sym) static void sym##_00(__VA_ARGS__, VALUE(*) (VALUE), int); \
                                                                    ^
2 warnings and 6 errors generated.

```

There is something wrong about the code and I suspect that scheduler contains garbage which is causing the method lookup failure/segfault.

Adding `#include <ruby/fiber/scheduler.h>` to your code will probably fix the issue.

#10 - 01/17/2024 08:28 AM - paddor (Patrik Wenger)

I knew it's something embarrassing like that. Adding `#include <ruby/fiber/scheduler.h>` actually helped. Thanks a lot.

#11 - 01/18/2024 05:38 PM - paddor (Patrik Wenger)

Unfortunately I still get the same error in the non-test project (not `fiber_blocker`). I've included `<ruby/fiber/scheduler.h>`. No compiler warnings regarding `rb_fiber_scheduler_*` but it still crashes when `rb_fiber_scheduler_unblock(scheduler, blocker, fiber)` is called. I even used a mutex `rb_mutex_new()` as the blocker object like in your example. I should be able to call `rb_fiber_scheduler_unblock()` from another (non-Ruby) thread, right?

#12 - 01/19/2024 09:45 PM - ioquatix (Samuel Williams)

Are you able to share the source code and error message? Thanks.