Ruby master - Bug #16907

Probable use-after-free in VM assertion

05/23/2020 02:10 AM - jeremyevans0 (Jeremy Evans)

Status:	Closed		
Priority:	Normal		
Assignee:	ko1 (Koichi Sasada)		
Target version:			
ruby -v:	ruby 2.8.0dev (2020-05-22) [x86_64-openbsd6.7]	**Backport:**	2.5: DONTNEED, 2.6: DONTNEED, 2.7: DONTNEED

Description

The following Ruby program fails with VM assertions enabled on OpenBSD (code taken from test_caller_to_enum in test/ruby/test_backtrace.rb):

```
      def foo
        return to_enum(__method__) unless block_given?
        raise
        yield 1
      end

      enum = foo
      enum.next
```

This is due to the following assertion in rb_current_vm in vm_core.h:

```
    VM_ASSERT(ruby_current_vm_ptr == NULL ||
              ruby_current_execution_context_ptr == NULL ||
              rb_ec_thread_ptr(GET_EC()) == NULL ||
              rb_ec_vm_ptr(GET_EC()) == ruby_current_vm_ptr);
```

Adding some debugging code, rb_ec_vm_ptr(GET_EC()) is 0xdfdfdfdfdfdfdfdf. This is the memory pattern that OpenBSD free(3) writes to memory in order to detect use-after-free. So it is quite likely that this is operating on freed memory.

My guess as to what is happening here is that the enumerator fiber stack is freed, but this VM assertion is still accessing the memory. However, that's just a guess, and not a particularly educated one. I am not sure how to fix it.

Associated revisions

Revision a0273d67 - 08/21/2020 09:52 PM - jeremyevans (Jeremy Evans)

Avoid a use after free in VM assertion

If the thread for the current EC has been killed, don't check
the VM ptr for the EC (which gets it via the thread), as that will
have already been freed.

Fixes [Bug #16907]

History

#1 - 08/21/2020 08:58 PM - jeremyevans0 (Jeremy Evans)

I think I've found a solution. If the thread for the EC has been killed, then don't check that the VM pointer matches, because the thread's memory (including the VM pointer) will have been freed. I've added a pull request that fixes this: https://github.com/ruby/ruby/pull/3443. This passes the bootstrap/basic tests on OpenBSD, which previously resulted in VM assertion failures without the change.

#2 - 08/21/2020 09:52 PM - jeremyevans (Jeremy Evans)

- Status changed from Open to Closed

Applied in changeset git|a0273d67d044dc9fe25313e0854a33374b990e8a.

Avoid a use after free in VM assertion

If the thread for the current EC has been killed, don't check

the VM ptr for the EC (which gets it via the thread), as that will have already been freed.

Fixes [Bug #16907]