# Ruby master - Bug #16771

**Segmentation fault when inspecting a bound method**

04/08/2020 10:32 PM - decuplet (Nikita Shilnikov)

<table>
<thead>
<tr>
<th>Status:</th>
<th>Open</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>ruby -v: 2.7.1</td>
</tr>
<tr>
<td>Backport:</td>
<td>2.5: UNKNOWN, 2.6: UNKNOWN, 2.7: REQUIRED</td>
</tr>
</tbody>
</table>

**Description**

This piece of code leads to a crash in ruby 2.7.1.

```ruby
bound_method = Kernel.instance_method(:respond_to?).bind(Object.new)
100000.times { bound_method.inspect }
```

I cannot reproduce the error in 2.7.0 so this must be new.

I attached the output, didn't bother with the crash report log, though. It should be easily reproducible since I found it on CI which runs a different OS.

**History**

#1 - 04/11/2020 12:51 AM - jeremyevans0 (Jeremy Evans)

I can reproduce this in 2.7.1, but not on master. Here's debugging information:

```
(gdb) bt
#0 0x00000bbf2523f290 in rb_funcallv_with_cc (cd=0xbbf25296430 <rb_inspect.rb_funcallv_data>, recv=12912719941280, mid=2753, argc=0, argv=0x0) at ./vm_eval.c:1012
#1 0x00000bbf2512f8cf in rb_inspect (objc=12912719941288) at object.c:680
#2 0x00000bbf251678cb in method_inspect (method=12913381588560) at proc.c:2854
#3 0x00000bbf2525014f in vm_call_cfunc_with_frame (ec=<optimized out>, reg_cfp=<optimized out>, calling=<optimized out>, cd=<optimized out>) at ./vm_insnhelper.c:2514
#4 vm_call_cfunc (ec=0xbbf3908ba50, reg_cfp=0xbbf3908ba50, calling=<optimized out>, cd=<optimized out>) at ./vm_insnhelper.c:2539
#5 0x00000bbf2523ae24 in vm_sendish (ec=<optimized out>, reg_cfp=<optimized out>, cd=0xbbf3908ba50, block_handler=0, method_explorer=<optimized out>) at ./vm_insnhelper.c:4023
#6 vm_exec_core (ec=<optimized out>, initial=<optimized out>) at insns.def:801
#7 0x00000bbf25244327 in vm_yield (ec=0xbbf25296430 <rb_inspect.rb_funcallv_data>, argc=1, argv=<optimized out>, kw_splat=0) at ./vm_insnhelper.c:1179
#8 rb_yield_0 (argc=1, argv=<optimized out>) at ./vm_eval.c:1227
#9 rb_yield_1 (val=<optimized out>) at ./vm_eval.c:1233
#10 0x00000bbf25129918 in int_dotimes (num=200001) at numeric.c:5201
#11 0x00000bbf2525014f in vm_call_cfunc_with_frame (ec=<optimized out>, reg_cfp=<optimized out>, calling=<optimized out>, cd=<optimized out>) at ./vm_insnhelper.c:2514
#12 vm_call_cfunc (ec=0xbbf3908ba50, reg_cfp=0xbbf3908ba50, calling=<optimized out>, cd=<optimized out>) at ./vm_insnhelper.c:2539
#13 0x00000bbf2523471b in vm_sendish (ec=<optimized out>, reg_cfp=<optimized out>, cd=0xbbf4722cef0, block_handler=<optimized out>) at ./vm_insnhelper.c:4023
#14 vm_exec_core (ec=0xbbf3908ba50, initial=<optimized out>) at insns.def:782
#15 0x00000bbf25244327 in vm_yield (ec=0xbbf25296430 <rb_inspect.rb_funcallv_data>, argc=1, argv=<optimized out>, kw_splat=0) at ./vm_insnhelper.c:1179
#16 rb_yield_0 (argc=1, argv=<optimized out>) at ./vm_eval.c:1227
#17 rb_yield_1 (val=<optimized out>) at ./vm_eval.c:1233
#18 0x00000bbf25129918 in int_dotimes (num=200001) at numeric.c:5201
#19 0x00000bbf2525014f in vm_call_cfunc_with_frame (ec=<optimized out>, reg_cfp=<optimized out>, calling=<optimized out>, cd=<optimized out>) at ./vm_insnhelper.c:2514
#20 vm_call_cfunc (ec=0xbbf3908ba50, reg_cfp=0xbbf3908ba50, calling=<optimized out>, cd=<optimized out>) at ./vm_insnhelper.c:2539
#21 0x00000bbf2523471b in vm_sendish (ec=<optimized out>, reg_cfp=<optimized out>, cd=0xbbf4722cef0, block_handler=<optimized out>, method_explorer=<optimized out>) at ./vm_insnhelper.c:4023
#22 vm_exec_core (ec=0xbbf3908ba50, initial=<optimized out>) at insns.def:782
#23 0x00000bbf25244327 in vm_yield (ec=0xbbf25296430 <rb_inspect.rb_funcallv_data>, argc=1, argv=<optimized out>, kw_splat=0) at ./vm_insnhelper.c:1179
#24 rb_yield_0 (argc=1, argv=<optimized out>) at ./vm_eval.c:1227
#25 rb_yield_1 (val=<optimized out>) at ./vm_eval.c:1233
#26 0x00000bbf25129918 in int_dotimes (num=200001) at numeric.c:5201
#27 0x00000bbf2525014f in vm_call_cfunc_with_frame (ec=<optimized out>, reg_cfp=<optimized out>, calling=<optimized out>, cd=<optimized out>) at ./vm_insnhelper.c:2514
#28 vm_call_cfunc (ec=0xbbf3908ba50, reg_cfp=0xbbf3908ba50, calling=<optimized out>, cd=<optimized out>) at ./vm_insnhelper.c:2539
#29 0x00000bbf2523471b in vm_sendish (ec=<optimized out>, reg_cfp=<optimized out>, cd=0xbbf4722cef0, block_handler=<optimized out>, method_explorer=<optimized out>) at ./vm_insnhelper.c:4023
#30 vm_exec_core (ec=0xbbf3908ba50, initial=<optimized out>) at insns.def:782
#31 0x00000bbf25244327 in vm_yield (ec=0xbbf25296430 <rb_inspect.rb_funcallv_data>, argc=1, argv=<optimized out>, kw_splat=0) at ./vm_insnhelper.c:1179
#32 rb_yield_0 (argc=1, argv=<optimized out>) at ./vm_eval.c:1227
#33 rb_yield_1 (val=<optimized out>) at ./vm_eval.c:1233
#34 0x00000bbf25129918 in int_dotimes (num=200001) at numeric.c:5201
#35 0x00000bbf2525014f in vm_call_cfunc_with_frame (ec=<optimized out>, reg_cfp=<optimized out>, calling=<optimized out>, cd=<optimized out>) at ./vm_insnhelper.c:2514
#36 vm_call_cfunc (ec=0xbbf3908ba50, reg_cfp=0xbbf3908ba50, calling=<optimized out>, cd=<optimized out>) at ./vm_insnhelper.c:2539
#37 0x00000bbf2523471b in vm_sendish (ec=<optimized out>, reg_cfp=<optimized out>, cd=0xbbf4722cef0, block_handler=<optimized out>, method_explorer=<optimized out>) at ./vm_insnhelper.c:4023
#38 vm_exec_core (ec=0xbbf3908ba50, initial=<optimized out>) at insns.def:782
#39 0x00000bbf25244327 in vm_yield (ec=0xbbf25296430 <rb_inspect.rb_funcallv_data>, argc=1, argv=<optimized out>, kw_splat=0) at ./vm_insnhelper.c:1179
#40 rb_yield_0 (argc=1, argv=<optimized out>) at ./vm_eval.c:1227
#41 rb_yield_1 (val=<optimized out>) at ./vm_eval.c:1233
#42 0x00000bbf25129918 in int_dotimes (num=200001) at numeric.c:5201
```

```
Cannot access memory at address 0x646f6874654d
```

#2 - 04/13/2020 02:18 AM - nagachika (Tomoyuki Chikanaga)

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