Ruby trunk - Bug #15382

Stack overflow in int_or()

12/05/2018 12:07 PM - fumfel (Kamil Frankowicz)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.6.0dev (2018-12-04 trunk 66199) [x86_64-linux]	**Backport:**	2.4: UNKNOWN, 2.5: UNKNOWN

Description

After some fuzz testing I found a crashing test case.

To reproduce: miniruby ruby_so_int_or

Full ASAN report: https://gist.github.com/fumfel/0a2e01f2ab6794632d017bfd306ffac9

ASAN report:

```
==22120==ERROR: AddressSanitizer: stack-overflow on address 0x7ffe9d1ddff8 (pc 0x55d12a2abd28 bp 0
x7ffe9d1de010 sp 0x7ffe9d1de000 T0)
    #0 0x55d12a2abd27 in int_or XYZ/ruby/numeric.c:4494
    #1 0x55d12a714ae7 in vm_call_cfunc_with_frame XYZ/ruby/./vm_insnhelper.c:1908:11
    #2 0x55d12a714ae7 in vm_call_cfunc XYZ/ruby/./vm_insnhelper.c:1924
    #3 0x55d12a69d73b in vm_exec_core XYZ/ruby/insns.def:766:5
    #4 0x55d12a6fc0ff in rb_vm_exec XYZ/ruby/vm.c:1876:22
    #5 0x55d12a6cf136 in vm_call0_body XYZ/ruby/./vm_eval.c:127:13
    #6 0x55d12a7387c1 in rb_vm_call0 XYZ/ruby/./vm_eval.c:60:12
    #7 0x55d12a7387c1 in call_method_entry XYZ/ruby/./vm_method.c:1954
    #8 0x55d12a6d2f89 in basic_obj_respond_to_missing XYZ/ruby/./vm_method.c:1971:12
    #9 0x55d12a6d2f89 in check_funcall_missing XYZ/ruby/./vm_eval.c:374
    #10 0x55d12a6d265e in rb_check_funcall_default XYZ/ruby/./vm_eval.c:420:14
    #11 0x55d12a28d664 in do_coerce XYZ/ruby/numeric.c:424:17
    #12 0x55d12a2ac03a in rb_num_coerce_bit XYZ/ruby/numeric.c:4424:5
    #13 0x55d12a2ac03a in fix_or XYZ/ruby/numeric.c:4489
    #14 0x55d12a2ac03a in int_or XYZ/ruby/numeric.c:4496
    [-------------------- SNIP ----------------------]
    #378 0x55d12a2ac03a in int_or XYZ/ruby/numeric.c:4496
    #379 0x55d12a714ae7 in vm_call_cfunc_with_frame XYZ/ruby/./vm_insnhelper.c:1908:11
    #380 0x55d12a714ae7 in vm_call_cfunc XYZ/ruby/./vm_insnhelper.c:1924
    #381 0x55d12a69d73b in vm_exec_core XYZ/ruby/insns.def:766:5
    #382 0x55d12a6fc0ff in rb_vm_exec XYZ/ruby/vm.c:1876:22
    #383 0x55d12a6cf136 in vm_call0_body XYZ/ruby/./vm_eval.c:127:13
    #384 0x55d12a7387c1 in rb_vm_call0 XYZ/ruby/./vm_eval.c:60:12
    #385 0x55d12a7387c1 in call_method_entry XYZ/ruby/./vm_method.c:1954
    #386 0x55d12a6d2f89 in basic_obj_respond_to_missing XYZ/ruby/./vm_method.c:1971:12
    #387 0x55d12a6d2f89 in check_funcall_missing XYZ/ruby/./vm_eval.c:374
    #388 0x55d12a6d265e in rb_check_funcall_default XYZ/ruby/./vm_eval.c:420:14

SUMMARY: AddressSanitizer: stack-overflow XYZ/ruby/numeric.c:4494 in int_or
==22120==ABORTING
```

Associated revisions

Revision 76e3af82 - 12/06/2018 11:06 PM - nobu (Nobuyoshi Nakada)

Warn redefinitions of some methods on Object

[Bug #5473] [Bug #14670] [Bug #15382]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@66262 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 66262 - 12/06/2018 11:06 PM - nobu (Nobuyoshi Nakada)

Warn redefinitions of some methods on Object

[Bug #5473] [Bug #14670] [Bug #15382]

Revision 66262 - 12/06/2018 11:06 PM - nobu (Nobuyoshi Nakada)

Warn redefinitions of some methods on Object

[Bug #5473] [Bug #14670] [Bug #15382]

History

#1 - 12/05/2018 01:04 PM - mame (Yusuke Endoh)

Briefly investigated. This is an infinite recursion.

Simplified version:

```
def respond_to_missing?(s, f)
  0 + "foo"
end
0.respond_to?(:foo)
```

0 + "foo" calls coerce, which calls respond_to_missing? recursively.

#2 - 12/05/2018 05:03 PM - nobu (Nobuyoshi Nakada)

Overwriting these methods also should be warned, as Object#initialize?

https://github.com/nobu/ruby/pull/new/bug/15382-warn-redef

#3 - 12/06/2018 11:06 PM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

Applied in changeset trunk|r66262.

Warn redefinitions of some methods on Object

[Bug #5473] [Bug #14670] [Bug #15382]

Files

ruby_so_int_or	59 Bytes	12/05/2018	fumfel (Kamil Frankowicz)