Ruby master - Bug #18458

Segmentation fault when missing Warning#warn method

01/04/2022 02:21 PM - etienne (Etienne Barrière)

<table>
<thead>
<tr>
<th>Status: Closed</th>
<th>Assignee: Normal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority: Normal</td>
<td>Target version: ruby -v: 3.1.0p0</td>
</tr>
<tr>
<td>Backport: 2.6: DONTNEED, 2.7: DONTNEED, 3.0: DONE, 3.1: DONE</td>
<td></td>
</tr>
</tbody>
</table>

Description

If you remove the Warning#warn method and call Kernel#warn, you get a segmentation fault:

```
ruby 3.1.0:
$ ruby -e 'Warning.undef_method(:warn); warn ""' 2>&1 | head -2

<internal:warning>:51: [BUG] Segmentation fault at 0x0000000000000010
ruby 3.1.0p0 (2021-12-25 revision fb4df44d16) [x86_64-darwin21]
```

It's not new, you get the same with 3.0.3:

```
ruby -e 'Warning.undef_method(:warn); warn ""' 2>&1 | head -2

<internal:warning>:51: [BUG] Segmentation fault at 0x0000000000000010
ruby 3.0.3p157 (2021-11-24 revision 3fb7d2cadc) [x86_64-darwin20]
```

In 2.7 though you get a NoMethodError exception:

```
$ ruby --disable-all -e 'Warning.undef_method(:warn); warn ""'
Traceback (most recent call last):
  1: from -e:1:in `<main>'
<internal:warning>:43:in `warn': undefined method `warn' for Warning:Module (NoMethodError)
```

(I disabled gems because rubygems core extensions adds two lines of backtrace, but it's the same result in the end)

Associated revisions

Revision 9e0a91d0 - 01/04/2022 06:03 PM - jeremyevans (Jeremy Evans)
Don't segfault if Warning.warn is undefined
Check that there is a method entry for the method before passing it to rb_method_entry_arity.
Fixes [Bug #18458]

Revision d3a2a3c5 - 01/30/2022 10:02 AM - naruse (Yui NARUSE)
merge revision(s) 9e0a91d0640600f2dfd7c1d5fae6667019c9ca5: [Backport #18458]

Don't segfault if Warning.warn is undefined
Check that there is a method entry for the method before passing it to rb_method_entry_arity.
Fixes [Bug #18458]

---
error.c | 3 ++-
test/ruby/test_exception.rb | 8 +++++++
2 files changed, 10 insertions(+), 1 deletion(-)

Revision e18e6af6 - 03/12/2022 07:53 AM - nagachika (Tomoyuki Chikanaga)
Don't segfault if Warning.warn is undefined

Check that there is a method entry for the method before passing it to rb_method_entry arity.

Fixes [Bug #18458]

---

| error.c | 3 ++- |
| test/ruby/test_exception.rb | 8 ++++++ |

2 files changed, 10 insertions(+), 1 deletion(-)

History

#1 - 01/04/2022 05:15 PM - jeremyevans0 (Jeremy Evans)
Pull requested submitted to fix this: https://github.com/ruby/ruby/pull/5391

#2 - 01/04/2022 05:42 PM - jeremyevans0 (Jeremy Evans)
- Backport changed from 2.6: UNKNOWN, 2.7: UNKNOWN, 3.0: UNKNOWN, 3.1: UNKNOWN to 2.6: DONTNEED, 2.7: DONTNEED, 3.0: REQUIRED, 3.1: REQUIRED

#3 - 01/04/2022 06:03 PM - jeremyevans (Jeremy Evans)
- Status changed from Open to Closed

Applied in changeset qit9e0a91d0640600f2dfd7c1d5fae6667019c9ca5.

Don't segfault if Warning.warn is undefined

Check that there is a method entry for the method before passing it to rb_method_entry arity.

Fixes [Bug #18458]

#4 - 01/30/2022 10:06 AM - naruse (Yui NARUSE)
- Backport changed from 2.6: DONTNEED, 2.7: DONTNEED, 3.0: REQUIRED, 3.1: REQUIRED to 2.6: DONTNEED, 2.7: DONTNEED, 3.0: REQUIRED, 3.1: DONE

ruby_3_1 d3a2a3c5420fecedee54cbf3bdd9287bc658f03 merged revision(s) 9e0a91d0640600f2dfd7c1d5fae6667019c9ca5.

#5 - 03/12/2022 07:57 AM - nagachika (Tomoyuki Chikanaga)
- Backport changed from 2.6: DONTNEED, 2.7: DONTNEED, 3.0: REQUIRED, 3.1: DONE to 2.6: DONTNEED, 2.7: DONTNEED, 3.0: DONE, 3.1: DONE

ruby_3_0 e186af604786be481115c7340c1450332615b57 merged revision(s) 9e0a91d0640600f2dfd7c1d5fae6667019c9ca5.