Ruby master - Bug #15087
Segmentation fault with splat and block
09/07/2018 02:58 PM - jacobevelyn (Jacob Evelyn)

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</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: 2.5.0, 2.5.1, 2.6.0dev (2018-09-07 trunk 64656)</td>
</tr>
<tr>
<td>Backport:</td>
<td>2.3: DONTNEED, 2.4: DONTNEED, 2.5: DONE</td>
</tr>
</tbody>
</table>

Description
The following code produces segmentation faults in Ruby 2.5.0, 2.5.1, and 2.6.0dev (2018-09-07 trunk 64656). This code worked in Ruby 2.4.1.

```ruby
test_proc = Proc.new { "test" }
def foo(bar: 1, &block)
  yield
end
foo(**{}, &test_proc)
```

I've attached the crash reports for both Ruby 2.6.0dev (2018-09-07 trunk 64656) and 2.5.1. Let me know if there's anything else I can provide.

Related issues:
- Related to Ruby master - Bug #15052: must not optimize `foo(**{})` out

Associated revisions
Revision d325d741 - 09/20/2018 01:43 AM - nobu (Nobuyoshi Nakada)
parse.y: fix block passing with empty kwargs
- parse.y (arg_blk_pass): preceeding arguments node may be NULL when an empty keyword argument hash splat is optimized away.
  [ruby-core:88890] [Bug #15087]
git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@64786 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 64786 - 09/20/2018 01:43 AM - nobu (Nobuyoshi Nakada)
parses.y: fix block passing with empty kwargs
- parse.y (arg_blk_pass): preceeding arguments node may be NULL when an empty keyword argument hash splat is optimized away.
  [ruby-core:88890] [Bug #15087]

Revision 64786 - 09/20/2018 01:43 AM - nobu (Nobuyoshi Nakada)
parses.y: fix block passing with empty kwargs
- parse.y (arg_blk_pass): preceeding arguments node may be NULL when an empty keyword argument hash splat is optimized away.
  [ruby-core:88890] [Bug #15087]

Revision a2d9317d - 11/06/2018 02:49 PM - nagachika (Tomoyuki Chikanaga)
merge revision(s) 64786: [Backport #15087]
parse.y: fix block passing with empty kwargs
- parse.y (arg_blk_pass): preceeding arguments node may be NULL when an empty keyword argument hash splat is optimized away.
  [ruby-core:88890] [Bug #15087]
git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_5@65579 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 65579 - 11/06/2018 02:49 PM - nagachika (Tomoyuki Chikanaga)
merge revision(s) 64786: [Backport #15087]
parse.y: fix block passing with empty kwargs

* parse.y (arg_blk_pass): preceeding arguments node may be NULL when an empty keyword argument hash splat is optimized away.
  [ruby-core:88890] [Bug #15087]

---

History

#1 - 09/07/2018 03:02 PM - mame (Yusuke Endoh)
- Related to Bug #15052: must not optimize `foo(**{})` out added

#2 - 09/07/2018 03:07 PM - mame (Yusuke Endoh)
Good catch. My patch for #15052 will fix this issue.

#3 - 09/20/2018 01:23 AM - mame (Yusuke Endoh)
mame (Yusuke Endoh) wrote:
  Good catch. My patch for #15052 will fix this issue.

We have never agreed with how to fix #15052 yet. Nobu is working on this issue without behavior change.

#4 - 09/20/2018 01:43 AM - nobu (Nobuyoshi Nakada)
- Status changed from Open to Closed

Applied in changeset trunk\r64786.

parse.y: fix block passing with empty kwargs

- parse.y (arg_blk_pass): preceeding arguments node may be NULL when an empty keyword argument hash splat is optimized away.  
  [ruby-core:88890] [Bug #15087]

#5 - 11/02/2018 07:31 PM - RubyBugs (A Nonymous)
This is still crashing in Ruby 2.5.3. Is this going to ever be fixed in Ruby 2.5 series?

#6 - 11/03/2018 05:35 AM - nobu (Nobuyoshi Nakada)
- Backport changed from 2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: UNKNOWN to 2.3: DONTNEED, 2.4: DONTNEED, 2.5: REQUIRED

Sorry, I've missed filling the Backport.

#7 - 11/06/2018 02:50 PM - nagachika (Tomoyuki Chikanaga)
- Backport changed from 2.3: DONTNEED, 2.4: DONTNEED, 2.5: REQUIRED to 2.3: DONTNEED, 2.4: DONTNEED, 2.5: DONE

ruby_2.5 r65579 merged revision(s) 64786.

#8 - 03/15/2019 06:37 PM - RubyBugs (A Nonymous)
Hurray! Confirmed that this no longer crashes and works as expected on 2.5.4 and 2.6.2

Files

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruby_2.6.0dev-2018-09-07-105158_Jacobs-MacBook-Pro.crash</td>
<td>36.4 KB</td>
<td>09/07/2018</td>
<td>jacobevelyn (Jacob Evelyn)</td>
</tr>
<tr>
<td>ruby_2.5.1-2018-09-07-105813_Jacobs-MacBook-Pro.crash</td>
<td>36.4 KB</td>
<td>09/07/2018</td>
<td>jacobevelyn (Jacob Evelyn)</td>
</tr>
</tbody>
</table>