Ruby master - Bug #10685

Segfault from keyword rest arg when coercing an object that defines to_hash

12/31/2014 11:39 PM - headius (Charles Nutter)

| Status: | Closed |
| Priority: | Normal |
| Assignee: | |
| Target version: | 2.2.0 |
| Backport: | 2.0.0: DONTNEED, 2.1: DONTNEED, 2.2: DONE |

Description

This spec appears to cause the segfault mentioned in [http://rubini.us/2014/12/31/matz-s-ruby-developers-don-t-use-rubyspec/](http://rubini.us/2014/12/31/matz-s-ruby-developers-don-t-use-rubyspec/) today.

```ruby
it "calls #to_hash on the last element if keyword arguments are present" do
  obj = mock("destructure block keyword arguments")
  obj.should_receive(:to_hash).and_return({x: 9})

  result = m([1, 2, 3, obj]) { |a, *b, c, **k| [a, b, c, k] }
  result.should == [1, [2], 3, {x: 9}]
end
```

I tried to boil it down to a shorter example and was not able to isolate it from RubySpec/mspec entanglement.

Here's the full dump including the last spec line that starts to run (the spec above): [https://gist.github.com/headius/5d52df923eb615729ca3](https://gist.github.com/headius/5d52df923eb615729ca3)

I ran it using mspec gem from rubyspec's "archive" branch using "mspec ci -f s language".

Related issues:

- Has duplicate Ruby master - Bug #10695: Segmentation fault with *args and **k...  Closed 01/04/2015
- Has duplicate Ruby master - Bug #10734: Segfault when combining default argum...  Closed 01/12/2015

Associated revisions

Revision abe15ddd - 01/01/2015 01:20 AM - nobu (Nobuyoshi Nakada)

```diff
+ vm_args.c: add ref r49088
  - vm_args.c (keyword_hash_p): fix non-symbol keys hash. rb_extract_keywords[] returns 0 not Qnil when no symbol keys is included. [ruby-core:67264] [Bug #10685]
```

Revision 49089 - 01/01/2015 01:20 AM - nobu (Nobuyoshi Nakada)

```diff
+ vm_args.c: add ref r49088
  - vm_args.c (keyword_hash_p): fix non-symbol keys hash. rb_extract_keywords[] returns 0 not Qnil when no symbol keys is included. [ruby-core:67264] [Bug #10685]
```

Revision 49089 - 01/01/2015 01:20 AM - nobu (Nobuyoshi Nakada)

```diff
+ vm_args.c: add ref r49088
  - vm_args.c (keyword_hash_p): fix non-symbol keys hash. rb_extract_keywords[] returns 0 not Qnil when no symbol keys is included. [ruby-core:67264] [Bug #10685]
```

Revision 49089 - 01/01/2015 01:20 AM - nobu (Nobuyoshi Nakada)

```diff
+ vm_args.c: add ref r49088
  - vm_args.c (keyword_hash_p): fix non-symbol keys hash. rb_extract_keywords[] returns 0 not Qnil when no symbol keys is included. [ruby-core:67264] [Bug #10685]
```

Revision 49089 - 01/01/2015 01:20 AM - nobu (Nobuyoshi Nakada)

```diff
+ vm_args.c: add ref r49088
  - vm_args.c (keyword_hash_p): fix non-symbol keys hash. rb_extract_keywords[] returns 0 not Qnil when no symbol keys is included. [ruby-core:67264] [Bug #10685]
```

Revision 49089 - 01/01/2015 01:20 AM - nobu (Nobuyoshi Nakada)

```diff
+ vm_args.c: add ref r49088
  - vm_args.c (keyword_hash_p): fix non-symbol keys hash. rb_extract_keywords[] returns 0 not Qnil when no symbol keys is included. [ruby-core:67264] [Bug #10685]
```
vm_args.c: add ref r49088

vm_args.c (keyword_hash_p): fix non-symbol keys hash. rb_extract_keywords() returns 0 not Qnil when no symbol keys is included.
[ruby-core:67264] [Bug #10685]

Revision 49089 - 01/01/2015 01:20 AM - nobu (Nobuyoshi Nakada)
vm_args.c: add ref r49088

vm_args.c (keyword_hash_p): fix non-symbol keys hash. rb_extract_keywords() returns 0 not Qnil when no symbol keys is included.
[ruby-core:67264] [Bug #10685]

Revision d40ee82b - 01/16/2015 05:03 AM - naruse (Yui NARUSE)
merge revision(s) 49089: [Backport #10685] included. [ruby-core:67264] [Bug #10685]
git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@49272 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 49272 - 01/16/2015 05:03 AM - naruse (Yui NARUSE)
merge revision(s) 49089: [Backport #10685] included. [ruby-core:67264] [Bug #10685]

Revision 81f257aa - 01/16/2015 05:21 AM - naruse (Yui NARUSE)
merge revision(s) 49088: [Backport #10685]

* vm_args.c (keyword_hash_p): fix non-symbol keys hash.
  rb_extract_keywords() returns 0 not Qnil when no symbol keys is included.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@49273 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 49273 - 01/16/2015 05:21 AM - naruse (Yui NARUSE)
merge revision(s) 49088: [Backport #10685]

* vm_args.c (keyword_hash_p): fix non-symbol keys hash.
  rb_extract_keywords() returns 0 not Qnil when no symbol keys is included.

History

#1 - 01/01/2015 12:14 AM - chrisseaton (Chris Seaton)
I think this is the equivalent code extracted from MSpec. But I can't get this to crash on 2.2.0p0.

def m(a) yield a end
class Mock
def to_hash
  puts 'to_hash called'
  {x: 9}
end
end

obj = Mock.new
result = m([1, 2, 3, obj]) { |a, *b, c, **k| [a, b, c, k] }
p result #.should == [1, [2], 3, {x: 9}]
p result == [1, [2], 3, {x: 9}]

#2 - 01/01/2015 12:38 AM - normalperson (Eric Wong)
Thanks for the report, looks like nobu committed a fix as r49088

This spec appears to cause the segfault mentioned in http://rubini.us/2014/12/31/matz-s-ruby-developers-don-t-use-rubyspec/ today.

Fwiw, I do run "make test-rubyspec" before I commit, but that's naruse's repo which I guess is different..

Like many projects nowadays, I won't bother contributing to rubyspec.
because it requires an account on a proprietary service provider.
Free Software (e.g. Ruby) needs Free tools:
http://mako.cc/writing/hill-free_tools.html

#3 - 01/01/2015 01:20 AM - nobu (Nobuyoshi Nakada)
- Status changed from Open to Closed
- % Done changed from 0 to 100

Applied in changeset r49089.

---

```
vm_args.c: add ref r49088

  * vm_args.c (keyword_hash_p): fix non-symbol keys hash. rb_extract_keywords() returns 0 not Qnil when no symbol keys is included.
  [ruby-core:67264] [Bug #10685]
```

#4 - 01/01/2015 01:25 AM - nobu (Nobuyoshi Nakada)
- Description updated
- Backport changed from 2.0.0: UNKNOWN, 2.1: UNKNOWN, 2.2: UNKNOWN to 2.0.0: DONTNEED, 2.1: DONTNEED, 2.2: REQUIRED

#5 - 01/01/2015 01:27 AM - nobu (Nobuyoshi Nakada)
Chris Seaton wrote:

> I think this is the equivalent code extracted from MSpec. But I can't get this to crash on 2.2.0p0.

It's another failure, but false positive.

#6 - 01/04/2015 04:11 PM - nobu (Nobuyoshi Nakada)
- Has duplicate Bug #10695: Segmentation fault with *args and **kwargs added

#7 - 01/12/2015 02:33 PM - ktsj (Kazuki Tsujimoto)
- Has duplicate Bug #10734: Segfault when combining default arguments with keyword arguments added

#8 - 01/16/2015 05:19 AM - naruse (Yui NARUSE)
- Backport changed from 2.0.0: DONTNEED, 2.1: DONTNEED, 2.2: REQUIRED to 2.0.0: DONTNEED, 2.1: DONTNEED, 2.2: DONE

ruby_2_2 r49272 merged revision(s) 49089.