Backport21 - Backport #9828

Segfault instead of stack overflow

05/11/2014 08:01 AM - plexus (Arne Brasseur)

<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>
</tbody>
</table>

**Description**
This causes a segmentation fault on 2.1.1 and 2.1.2, instead of SystemStackError

```ruby
define_method(:foo) { send(:foo) }
foo
```

**Related issues:**
Is duplicate of Ruby master - Bug #9454: The define_method(class) segfault

**Associated revisions**

**Revision ced638cc - 06/19/2014 03:56 PM - nagachika (Tomoyuki Chikanaga)**
merge revision(s) r44712,r44715,r44716,r44722,r44725,r44726,r44753: [Backport #9454] [Backport #9828]

- thread_pthread.c: get current main thread stack size, which may be expanded than allocated size at initialization, by rlimit().
  [ruby-core:60113] [Bug #9454]

- thread_pthread.c: rlimit is only available on Linux.
  At least r44712 breaks FreeBSD.
  [ruby-core:60113] [Bug #9454]

- thread_pthread.c (ruby_init_stack, ruby_stack_overflowed_p):
  place get_stack above others to get stack boundary information.
  [ruby-core:60113] [Bug #9454]

**Revision 46468 - 06/19/2014 03:56 PM - nagachika (Tomoyuki Chikanaga)**
merge revision(s) r44712,r44715,r44716,r44722,r44725,r44726,r44753: [Backport #9454] [Backport #9828]

- thread_pthread.c: get current main thread stack size, which may be expanded than allocated size at initialization, by rlimit().
  [ruby-core:60113] [Bug #9454]

- thread_pthread.c: rlimit is only available on Linux.
  At least r44712 breaks FreeBSD.
  [ruby-core:60113] [Bug #9454]

- thread_pthread.c (ruby_init_stack, ruby_stack_overflowed_p):
  place get_stack above others to get stack boundary information.
  [ruby-core:60113] [Bug #9454]

**History**

#1 - 05/12/2014 03:31 AM - nobu (Nobuyoshi Nakada)
- Tracker changed from Bug to Backport
- Project changed from Ruby master to Backport21
- Description updated
- Category deleted (core)

SystemStackError on trunk.

#2 - 05/27/2014 03:18 AM - hsbt (Hiroshi SHIBATA)
nobu

Do you know which commits related to this issue?
The test for it was introduced at r44712, but many changes are in thread*.c and signal.c then.

- Is duplicate of Bug #9454: The define_method(:class) segfault added

- Status changed from Open to Closed
- % Done changed from 0 to 100

Applied in changeset r46468.

merge revision(s) r44712,r44715,r44716,r44722,r44725,r44726,r44753: [Backport #9454] [Backport #9828]

* thread_pthread.c: get current main thread stack size, which may be expanded than allocated size at initialization, by rlimit().
  [ruby-core:60113] [Bug #9454]

* thread_pthread.c: rlimit is only available on Linux.
  At least r44712 breaks FreeBSD.
  [ruby-core:60113] [Bug #9454]

* thread_pthread.c (ruby_init_stack, ruby_stack_overflowed_p):
  place get_stack above others to get stack boundary information.
  [ruby-core:60113] [Bug #9454]