

Ruby - Bug #1548

Segfault when Transferring to a Fiber which Resumes Itself

06/01/2009 06:16 AM - runpaint (Run Paint Run Run)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 1.9.2dev (2009-05-28 trunk 23601) [i686-linux]	Backport:

Description

=begin

On both the trunk version and 1.9.1 I can reproduce a segfault by transferring to a Fiber from the root Fiber, when the former attempts to resume itself. Both stack traces below were generated from binaries I compiled myself using the default flags.

\$ rubybleed -rfiber -e 'f=Fiber.new{f.resume};f.transfer'

[BUG] Segmentation fault

ruby 1.9.2dev (2009-05-28 trunk 23601) [i686-linux]

-- control frame -----

c:0001 p:---- s:0001 b:-001 l:000000 d:000000 -----

-- C level backtrace information -----

rubybleed(rb_vm_bugreport+0xb5) [0x8160615]

rubybleed [0x819b51b]

rubybleed(rb_bug+0x28) [0x819b5a8]

rubybleed [0x80f5645]

[0xb7f04410]

rubybleed [0x805f0c1]

rubybleed [0x805f503]

rubybleed [0x819bae5]

rubybleed(rb_fiber_transfer+0xfb) [0x816934b]

rubybleed(rb_fiber_start+0x147) [0x81694b7]

rubybleed [0x805cfde]

rubybleed(ruby_run_node+0x46) [0x805e8a6]

rubybleed(main+0x60) [0x805c3d0]

/lib/tls/i686/cmov/libc.so.6(__libc_start_main+0xe5) [0xb7d25775]

rubybleed [0x805c2d1]

[NOTE]

You may have encountered a bug in the Ruby interpreter or extension libraries.

Bug reports are welcome.

For details: <http://www.ruby-lang.org/bugreport.html>

Aborted

\$ ruby91 -rfiber -e 'f=Fiber.new{f.resume};f.transfer'

[BUG] Segmentation fault

ruby 1.9.1p154 (2009-05-22 revision 23541) [i686-linux]

-- control frame -----

c:0001 p:---- s:0001 b:-001 l:000000 d:000000 -----

-- Ruby level backtrace information-----

-- C level backtrace information -----

0x812d908 ruby91(rb_vm_bugreport+0x48) [0x812d908]

0x815bed1 ruby91 [0x815bed1]

0x815bf48 ruby91(rb_bug+0x28) [0x815bf48]

0x80d90b6 ruby91 [0x80d90b6]

```
0xb8048410 [0xb8048410]
0x805cd49 ruby91 [0x805cd49]
0x805d113 ruby91 [0x805d113]
0x815b2bf ruby91 [0x815b2bf]
0x8133dcb ruby91(rb_fiber_transfer+0xfb) [0x8133dcb]
0x8133f9b ruby91(rb_fiber_start+0x14b) [0x8133f9b]
0x805d386 ruby91 [0x805d386]
0x805e8a6 ruby91(ruby_run_node+0x46) [0x805e8a6]
0x805bea0 ruby91(main+0x60) [0x805bea0]
0xb7e69775 /lib/tls/i686/cmov/libc.so.6(__libc_start_main+0xe5) [0xb7e69775]
0x805bda1 ruby91 [0x805bda1]
```

[NOTE]

You may encounter a bug of Ruby interpreter. Bug reports are welcome.

For details: <http://www.ruby-lang.org/bugreport.html>

Aborted

=end

History

#1 - 06/01/2009 11:27 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

- % Done changed from 0 to 100

=begin

Applied in changeset r23616.

=end