Backport191 - Bug #1856

[BUG] Segmentation fault in 1.9.1p149

08/01/2009 10:25 PM - anthonywright (Anthony Wright)

Status:	Feedback
Priority:	Normal
Assignee:	
Target version:	
ruby -v:	ruby 1.9.1p129 (2009-05-12 revision 23412) [i686-linux]

Description

=begin
I have a 120 line pure ruby application that bombs out in 1.9.1p129 after 1-2 seconds with a [BUG] Segmentation fault & [BUG] object allocation during garbage collection phase.

I'm using a piece of code that I got from Ruby Treasures which has worked fine in 1.8.X for a long time. I'm going through the process of porting to 1.9.1. I've inlined this code, and my little app that uses it is at the bottom.

The error output I see is:

seg-fault.rb:115: [BUG] Segmentation fault
ruby 1.9.1p129 (2009-05-12 revision 23412) [i686-linux]

-- control frame ----------
c:0008 p:---- s:0040 b:0040 l:000039 d:000039 CFUNC :readlines
c:0007 p:0011 s:0037 b:0037 l:00157c d:000036 BLOCK seg-fault.rb:115
c:0006 p:0014 s:0032 b:0032 l:000014 d:000031 BLOCK seg-fault.rb:95
c:0005 p:0272 s:0026 b:0026 l:000025 d:000025 METHOD seg-fault.rb:78
c:0004 p:0024 s:0015 b:0015 l:000014 d:000014 METHOD seg-fault.rb:94
c:0003 p:0045 s:0006 b:0006 l:00157c d:001f8c EVAL   seg-fault.rb:114
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:00157c d:00157c TOP   :17

---

seg-fault.rb:115: [BUG] object allocation during garbage collection phase
ruby 1.9.1p129 (2009-05-12 revision 23412) [i686-linux]

-- control frame ----------
c:0008 p:---- s:0040 b:0040 l:000039 d:000039 CFUNC :readlines
c:0007 p:0011 s:0037 b:0037 l:00157c d:000036 BLOCK seg-fault.rb:115
c:0006 p:0014 s:0032 b:0032 l:000014 d:000031 BLOCK seg-fault.rb:95
c:0005 p:0272 s:0026 b:0026 l:000025 d:000025 METHOD seg-fault.rb:78
c:0004 p:0024 s:0015 b:0015 l:000014 d:000014 METHOD seg-fault.rb:94
c:0003 p:0045 s:0006 b:0006 l:00157c d:001f8c EVAL   seg-fault.rb:114
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:00157c d:00157c TOP   :17

-- Ruby level backtrace information--
seg-fault.rb:115:in readlines'
seg-fault.rb:115:inblock in '
seg-fault.rb:95:in block in popen3'
seg-fault.rb:78:inpopen3_with_pid'
seg-fault.rb:94:in popen3'
seg-fault.rb:114:in'

-- C level backtrace information ---

[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 - 08/01/2009 11:35 PM - anthonywright (Anthony Wright)

=begin
Oops, I think I'm finding bugs in versions that haven't even been released yet! As I said elsewhere in the post I meant 1.9.1p129...
=end

#2 - 08/01/2009 11:38 PM - rogerdpack (Roger Pack)

=begin
have you tried it with ruby trunk?
=end

#3 - 08/02/2009 12:09 AM - phasis68 (Heesob Park)

=begin
I think this segmentation fault is due to the bug of your code.

Here is a patch for your code seg-fault.rb:
@@ -42,7 +42,7 @@
rd[1].close ; STDIN .reopen(rd[0]) ; rd[0].close
wr[0].close ; STDOUT.reopen(wr[1]) ; wr[1].close
err[0].close ; STDERR.reopen(err[1]) ; err[1].close
-

- ps[0].close begin exec(*cmd) raise "exec returned!" @@ -66,7 +66,7 @@ rescue EOFError # If we get an EOF error, then the exec was successful. end -
- ps[0].close # If exc is set, then the exec was NOT successful. if not exc.nil? then raise exc

=end

#4 - 04/10/2010 11:54 AM - mame (Yusuke Endoh)

- Status changed from Open to Feedback

=begin
Hi,

2009/8/1 Anthony Wright redmine@ruby-lang.org:

> I have a 120 line pure ruby application that bombs out in 1.9.1p129 after 1-2 seconds with a [BUG] Segmentation fault & [BUG] object allocation during garbage collection phase.
>
> I'm using a piece of code that I got from Ruby Treasures which has worked fine in 1.8.X for a long time. I'm going through the process of porting to 1.9.1. I've inlined this code, and my little app that uses it is at the bottom.

Thank you for report.
But I cannot reproduce with both ruby 1.9.1p129 and trunk.
Can anyone reproduce?

I guess this bug may depend on gcc's optimization.
Could you tell us how did you build ruby?

--
Yusuke ENDOH mame@tsg.ne.jp
=end

Files

seg-fault.rb	2.91 KB	08/01/2009	anthonywright (Anthony Wright)