

Ruby - Bug #2558

r24591 causes Segfault

01/05/2010 06:28 PM - a3li (Alex Legler)

Status: Closed		Backport:
Priority: Normal		
Assignee:		
Target version:		
ruby -v:	ruby 1.9.1p376 (2009-12-07 revision 26041) [x86_64-linux]	
Description		
<pre>=begin</pre> While looking into a test failure in test_thread.rb (ticket #2506), I stumbled upon a segmentation fault that was randomly happening. To reproduce, run make test', or the extracted sample (attached) while redirecting output. i.e. ./ruby19 ~/reprod.rb > /dev/null' multiple times, until randomly a segv occurs. The segfault only seems to occur on systems with a glibc >= 2.10, I reproduced it on Gentoo x86 with glibc 2.10 and amd64 with glibc 2.11. I "bisected" my way through the changes between 1.9.1_p243 and 1.9.1_p376 and found that r24591 (applied in the 1_9_1 branch in r25539) is the cause. If I take a pristine p376 snapshot and just revert the aforementioned change, the issue goes away. This is what the crash output looks like: <pre>--</pre> /home/alex/file.rb:114: [BUG] Segmentation fault ruby 1.9.1p376 (2009-12-07 revision 26041) [x86_64-linux] <pre>-- control frame -----</pre> c:0003 p:0000 s:0007 b:0007 l:001f88 d:000006 BLOCK /home/alex/file.rb:114 c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH c:0001 p:---- s:0002 b:0002 l:000001 d:000001 TOP <pre>-- Ruby level backtrace information-----</pre> /home/alex/file.rb:114:in `block (2 levels) in ' <pre>-- C level backtrace information -----</pre> 0x7f8e9a8443d1 ./libruby19.so.1.9(rb_vm_bugreport+0x51) [0x7f8e9a8443d1] 0x7f8e9a76caae ./libruby19.so.1.9(+0x50aae) [0x7f8e9a76caae] 0x7f8e9a76cc13 ./libruby19.so.1.9(rb_bug+0xb3) [0x7f8e9a76cc13] 0x7f8e9a7eebb5 ./libruby19.so.1.9(+0xd2bb5) [0x7f8e9a7eebb5] 0x7f8e9a50f010 /lib/libpthread.so.0(+0xf010) [0x7f8e9a50f010] 0x72e6e0 [0x72e6e0] [NOTE] You may encounter a bug of Ruby interpreter. Bug reports are welcome. For details: http://www.ruby-lang.org/bugreport.html Note that file.rb is what I attach as reprod.rb and does not have 114 lines! Please also find more info from gdb attached. <pre>=end</pre>		
Related issues:		
Related to Ruby - Bug #1813: Threading seg fault (1.9.1-p129 Linux/Mac)		Closed 07/24/2009
Related to Ruby - Feature #1952: cannot stop with Ctrl+C		Closed 08/18/2009

History

#1 - 01/05/2010 07:35 PM - naruse (Yui NARUSE)

- Status changed from Open to Assigned
- Assignee set to yugui (Yuki Sonoda)

=begin

=end

#2 - 01/27/2010 09:43 AM - rogerdpack (Roger Pack)

=begin
do you get this with trunk?
=end

#3 - 01/27/2010 04:53 PM - naruse (Yui NARUSE)

- Category set to core
- Status changed from Assigned to Open
- Assignee deleted (yugui (Yuki Sonoda))

=begin
Can't reproduce at r26358, but Now can reproduce on ruby 1.9.2dev (2010-01-27 trunk 26434) [x86_64-freebsd8.0]
=end

#4 - 01/28/2010 06:08 AM - a3li (Alex Legler)

=begin
trunk: ruby 1.9.2dev (2010-01-28 trunk 26454) [x86_64-linux]

```
alex@neon trunk % ./ruby ~/file.rb >| /dev/null
*** glibc detected *** ./ruby: free(): corrupted unsorted chunks: 0x000000000080daa0 ***
===== Backtrace: =====
/lib/libc.so.6(+0x72406)[0x7f98421b9406]
/lib/libc.so.6(cfree+0x6c)[0x7f98421be1ac]
./ruby(rb_objspace_free+0x86)[0x422e36]
./ruby(ruby_vm_destruct+0x8d)[0x5045ed]
./ruby(ruby_cleanup+0x196)[0x41bb36]
./ruby(ruby_run_node+0x3d)[0x41bd2d]
./ruby(main+0x49)[0x419349]
/lib/libc.so.6(__libc_start_main+0xfd)[0x7f9842165bbd]
./ruby[0x419239]
===== Memory map: =====
00400000-005f2000 r-xp 00000000 fc:00 193267                /home/alex/trash/ruby-traunk/trunk/ruby
007f1000-007f2000 r--p 001f1000 fc:00 193267                /home/alex/trash/ruby-traunk/trunk/ruby
007f2000-007f4000 rw-p 001f2000 fc:00 193267                /home/alex/trash/ruby-traunk/trunk/ruby
007f4000-0097a000 rw-p 00000000 00:00 0                    [heap]
7f9834000000-7f9834021000 rw-p 00000000 00:00 0
7f9834021000-7f9838000000 ---p 00000000 00:00 0
7f9838614000-7f983862a000 r-xp 00000000 09:01 5831          /lib64/libgcc_s.so.1
7f983862a000-7f9838829000 ---p 00016000 09:01 5831          /lib64/libgcc_s.so.1
7f9838829000-7f983882a000 r--p 00015000 09:01 5831          /lib64/libgcc_s.so.1
7f983882a000-7f983882b000 rw-p 00016000 09:01 5831          /lib64/libgcc_s.so.1
7f983882b000-7f983882c000 ---p 00000000 00:00 0
7f983882c000-7f98388ac000 rw-p 00000000 00:00 0
7f98389ad000-7f98389ae000 ---p 00000000 00:00 0
7f98389ae000-7f9838a2e000 rw-p 00000000 00:00 0
7f9838b2f000-7f9838b30000 ---p 00000000 00:00 0
7f9838b30000-7f9838bb0000 rw-p 00000000 00:00 0
7f9838cb1000-7f9838cb2000 ---p 00000000 00:00 0
7f9838cb2000-7f9838d32000 rw-p 00000000 00:00 0
7f9838e33000-7f9838e34000 ---p 00000000 00:00 0
7f9838e34000-7f9838eb4000 rw-p 00000000 00:00 0
7f9838fb5000-7f9838fb6000 ---p 00000000 00:00 0
7f9838fb6000-7f9839036000 rw-p 00000000 00:00 0
7f9839137000-7f9839138000 ---p 00000000 00:00 0
7f9839138000-7f98391b8000 rw-p 00000000 00:00 0
7f98392b9000-7f98392ba000 ---p 00000000 00:00 0
7f98392ba000-7f983933a000 rw-p 00000000 00:00 0
7f983943b000-7f983943c000 ---p 00000000 00:00 0
7f983943c000-7f98394bc000 rw-p 00000000 00:00 0
7f98395bd000-7f98395be000 ---p 00000000 00:00 0
7f98395be000-7f983963e000 rw-p 00000000 00:00 0
```

7f983973f000-7f9839740000 ---p 00000000 00:00 0
7f9839740000-7f98397c0000 rw-p 00000000 00:00 0
7f98398c1000-7f98398c2000 ---p 00000000 00:00 0
7f98398c2000-7f9839942000 rw-p 00000000 00:00 0
7f9839a43000-7f9839a44000 ---p 00000000 00:00 0
7f9839a44000-7f9839ac4000 rw-p 00000000 00:00 0
7f9839bc5000-7f9839bc6000 ---p 00000000 00:00 0
7f9839bc6000-7f9839c46000 rw-p 00000000 00:00 0
7f9839d47000-7f9839d48000 ---p 00000000 00:00 0
7f9839d48000-7f9839dc8000 rw-p 00000000 00:00 0
7f9839ec9000-7f9839eca000 ---p 00000000 00:00 0
7f9839eca000-7f9839f4a000 rw-p 00000000 00:00 0
7f983a04b000-7f983a04c000 ---p 00000000 00:00 0
7f983a04c000-7f983a0cc000 rw-p 00000000 00:00 0
7f983a1cd000-7f983a1ce000 ---p 00000000 00:00 0
7f983a1ce000-7f983a24e000 rw-p 00000000 00:00 0
7f983a34f000-7f983a350000 ---p 00000000 00:00 0
7f983a350000-7f983a3d0000 rw-p 00000000 00:00 0
7f983a4d1000-7f983a4d2000 ---p 00000000 00:00 0
7f983a4d2000-7f983a552000 rw-p 00000000 00:00 0
7f983a653000-7f983a654000 ---p 00000000 00:00 0
7f983a654000-7f983a7d5000 rw-p 00000000 00:00 0
7f983a7d5000-7f983a7d6000 ---p 00000000 00:00 0
7f983a7d6000-7f983a957000 rw-p 00000000 00:00 0
7f983a957000-7f983a958000 ---p 00000000 00:00 0
7f983a958000-7f983aad9000 rw-p 00000000 00:00 0
7f983aad9000-7f983aada000 ---p 00000000 00:00 0
7f983aada000-7f983ac5b000 rw-p 00000000 00:00 0
7f983ac5b000-7f983ac5c000 ---p 00000000 00:00 0
7f983ac5c000-7f983acdc000 rw-p 00000000 00:00 0
7f983addd000-7f983adde000 ---p 00000000 00:00 0
7f983adde000-7f983af5f000 rw-p 00000000 00:00 0
7f983af5f000-7f983af60000 ---p 00000000 00:00 0
7f983af60000-7f983b0e1000 rw-p 00000000 00:00 0
7f983b0e1000-7f983b0e2000 ---p 00000000 00:00 0
7f983b0e2000-7f983b263000 rw-p 00000000 00:00 0
7f983b263000-7f983b264000 ---p 00000000 00:00 0
7f983b264000-7f983b3e5000 rw-p 00000000 00:00 0
7f983b3e5000-7f983b3e6000 ---p 00000000 00:00 0
7f983b3e6000-7f983b567000 rw-p 00000000 00:00 0
7f983b567000-7f983b568000 ---p 00000000 00:00 0
7f983b568000-7f983b6e9000 rw-p 00000000 00:00 0
7f983b6e9000-7f983b6ea000 ---p 00000000 00:00 0
7f983b6ea000-7f983b76a000 rw-p 00000000 00:00 0
7f983b86b000-7f983b86c000 ---p 00000000 00:00 0
7f983b86c000-7f983b8ec000 rw-p 00000000 00:00 0
7f983b9ed000-7f983b9ee000 ---p 00000000 00:00 0
7f983b9ee000-7f983bb6f000 rw-p 00000000 00:00 0
7f983bb6f000-7f983bb70000 ---p 00000000 00:00 0
7f983bb70000-7f983bcf1000 rw-p 00000000 00:00 0
7f983bd72000-7f983be73000 rw-p 00000000 00:00 0
7f983bef4000-7f983bff5000 rw-p 00000000 00:00 0
7f983c076000-7f983c177000 rw-p 00000000 00:00 0
7f983c1f8000-7f983c2f9000 rw-p 00000000 00:00 0
7f983c37a000-7f983c47b000 rw-p 00000000 00:00 0
7f983c47b000-7f983c47c000 ---p 00000000 00:00 0
7f983c47c000-7f983c5fd000 rw-p 00000000 00:00 0
7f983c67e000-7f983c77f000 rw-p 00000000 00:00 0
7f983c77f000-7f983c780000 ---p 00000000 00:00 0
7f983c780000-7f983c901000 rw-p 00000000 00:00 0
7f983c982000-7f983ca83000 rw-p 00000000 00:00 0
7f983ca83000-7f983ca84000 ---p 00000000 00:00 0
7f983ca84000-7f983cc05000 rw-p 00000000 00:00 0
7f983cc05000-7f983cc06000 ---p 00000000 00:00 0
7f983cc06000-7f983cc86000 rw-p 00000000 00:00 0
7f983cd87000-7f983cd88000 ---p 00000000 00:00 0
7f983cd88000-7f983ce08000 rw-p 00000000 00:00 0
7f983cf09000-7f983cf0a000 ---p 00000000 00:00 0
7f983cf0a000-7f983d08b000 rw-p 00000000 00:00 0
7f983d08b000-7f983d08c000 ---p 00000000 00:00 0
7f983d08c000-7f983d20d000 rw-p 00000000 00:00 0
7f983d20d000-7f983d20e000 ---p 00000000 00:00 0
7f983d20e000-7f983d38f000 rw-p 00000000 00:00 0
7f983d38f000-7f983d390000 ---p 00000000 00:00 0
7f983d390000-7f983d511000 rw-p 00000000 00:00 0

7f983d511000-7f983d512000 ---p 00000000 00:00 0
7f983d512000-7f983d693000 rw-p 00000000 00:00 0
7f983d693000-7f983d694000 ---p 00000000 00:00 0
7f983d694000-7f983d815000 rw-p 00000000 00:00 0
7f983d815000-7f983d816000 ---p 00000000 00:00 0
7f983d816000-7f983d997000 rw-p 00000000 00:00 0
7f983d997000-7f983d998000 ---p 00000000 00:00 0
7f983d998000-7f983db19000 rw-p 00000000 00:00 0
7f983db19000-7f983db1a000 ---p 00000000 00:00 0
7f983db1a000-7f983dc9b000 rw-p 00000000 00:00 0
7f983dc9b000-7f983dc9c000 ---p 00000000 00:00 0
7f983dc9c000-7f983de1d000 rw-p 00000000 00:00 0
7f983de1d000-7f983de1e000 ---p 00000000 00:00 0
7f983de1e000-7f983df9f000 rw-p 00000000 00:00 0
7f983df9f000-7f983dfa0000 ---p 00000000 00:00 0
7f983dfa0000-7f983e121000 rw-p 00000000 00:00 0
7f983e121000-7f983e122000 ---p 00000000 00:00 0
7f983e122000-7f983e1a2000 rw-p 00000000 00:00 0
7f983e2a3000-7f983e2a4000 ---p 00000000 00:00 0
7f983e2a4000-7f983e425000 rw-p 00000000 00:00 0
7f983e425000-7f983e426000 ---p 00000000 00:00 0
7f983e426000-7f983e5a7000 rw-p 00000000 00:00 0
7f983e5a7000-7f983e5a8000 ---p 00000000 00:00 0
7f983e5a8000-7f983e729000 rw-p 00000000 00:00 0
7f983e729000-7f983e72a000 ---p 00000000 00:00 0
7f983e72a000-7f983e8ab000 rw-p 00000000 00:00 0
7f983e8ab000-7f983e8ac000 ---p 00000000 00:00 0 [1] 19653 abort (core dumped) ./ruby ~/file.rb >| /dev/null

=end

#5 - 04/19/2010 10:08 PM - mame (Yusuke Endoh)

=begin
Hi,

The original reporter is right.
r24591 must be reverted. I'll do.

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

#6 - 04/28/2010 10:57 PM - mame (Yusuke Endoh)

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

=begin
This issue was solved with changeset r27534.
Alex, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

=end

Files

reprod.rb	171 Bytes	01/05/2010	a3li (Alex Legler)
ruby-backtrace.txt	98.4 KB	01/05/2010	a3li (Alex Legler)