Ruby trunk - Bug #11567

Segmentation fault CFUNC :gets

10/05/2015 05:23 PM - dmitry_uk (D R)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.2.3p173 (2015-08-18 revision 51636) [x86_64-linux]	**Backport:**	2.0.0: UNKNOWN, 2.1: UNKNOWN, 2.2: UNKNOWN

Description

Running the below code under 2.2.3 results in a segmentation fault. Runs without issue on 2.1.6. Output attached as a text file.

```
require 'open3'
require 'pp'

data_accessor = Mutex.new
results = {}
threads = []

200.times.each do |i|
  threads << Thread.new do
    Open3.popen3('ping localhost -c 2') do |_stdin, stdout, stderr, thread|

      { out: stdout, err: stderr }.each do |key, stream|
        t = "#{i}-" + key.to_s
        data_accessor.synchronize do
          results[t] = []
        end
        Thread.new do
          until (line = stream.gets).nil?
            data_accessor.synchronize do
              results[t].push line
            end
          end
        end
      end

      thread.join
    end
  end
end

threads.each(&:join)

pp results
```

History

#1 - 05/07/2016 12:56 AM - hsbt (Hiroshi SHIBATA)

- Description updated

- Status changed from Open to Feedback

I couldn't reproduce this with latest versions of 2.1-2.4.

Please try with 2.2.5 or 2.3.1.

#2 - 02/17/2017 11:00 AM - nh_cham (Michael Specht)

I'm having the same problem. Running the code as it is, I get reproducible crashes with both Ruby 2.3.1 and 2.4.0:

```
test.rb:18: [BUG] Segmentation fault at 0x00000000000000
```

```
ruby 2.4.0p0 (2016-12-24 revision 57164) [x86_64-linux]

-- Control frame information -----------------------------------------------
c:0003 p:---- s:0011 e:000010 CFUNC  :gets
c:0002 p:0027 s:0007 e:000006 BLOCK  test.rb:18 [FINISH]
c:0001 p:---- s:0003 e:000002 (none) [FINISH]

test.rb:18: [BUG] Segmentation fault at 0x00000000000000
ruby 2.3.1p112 (2016-04-26) [x86_64-linux-gnu]

-- Control frame information -----------------------------------------------
c:0003 p:---- s:0008 e:000007 CFUNC  :gets
c:0002 p:0027 s:0005 e:000004 BLOCK  test.rb:18 [FINISH]
c:0001 p:---- s:0002 e:000001 (none) [FINISH]
```

I can't even get the complete output or Ctrl+C out of it, because my shell hangs after that (two different systems), but it helps to kill -9 the Ruby process.

#3 - 03/10/2017 02:08 PM - nobu (Nobuyoshi Nakada)

- Description updated

I can't reproduce it, but it seems [Bug #13076].

#4 - 04/18/2017 04:31 AM - shyouhei (Shyouhei Urabe)

- Status changed from Feedback to Closed

It seems fixed already. Try a newer version. Tell us if it still happens.

Files

gets bug.txt	30.7 KB	10/05/2015	dmitry_uk (D R)