Ruby master - Bug #3784

Seg fault in IO.select from webrick

09/03/2010 06:08 AM - enrico (Enrico Brunetta)

Status:	Closed		
Priority:	Normal		
Assignee:	nahi (Hiroshi Nakamura)		
Target version:			
ruby -v:	ruby 1.9.2p0 (2010-08-18 revision 29036) [x86_64-darwin10.4.0]	**Backport:**	

Description

I get this intermittently (approximately once a day) on my OSX 10.6.4. I have used rvm to install 1.9.2-p0

```
/usr/local/Cellar/ruby/1.9.2-p0/lib/ruby/1.9.1/webrick/server.rb:90: [BUG] Segmentation fault
ruby 1.9.2p0 (2010-08-18 revision 29036) [x86_64-darwin10.4.0]

-- control frame ----------
c:0012 p:---- s:0055 b:0055 l:000054 d:000054 CFUNC  :select
c:0011 p:0106 s:0048 b:0048 l:000038 d:000047 BLOCK  /usr/local/Cellar/ruby/1.9.2-p0/lib/ruby/1.9.
1/webrick/server.rb:90
c:0010 p:0007 s:0042 b:0042 l:000041 d:000041 METHOD /usr/local/Cellar/ruby/1.9.2-p0/lib/ruby/1.9.
1/webrick/server.rb:22
c:0009 p:0063 s:0039 b:0039 l:000038 d:000038 METHOD /usr/local/Cellar/ruby/1.9.2-p0/lib/ruby/1.9.
1/webrick/server.rb:81
c:0008 p:0126 s:0034 b:0034 l:001f90 d:001f90 METHOD /usr/local/Cellar/ruby/1.9.2-p0/lib/ruby/gems
/1.9.1/gems/rack-1.1.0/lib/rack/handler/webrick.rb:14
c:0007 p:0806 s:0028 b:0028 l:0001b0 d:0001b0 TOP    /usr/local/Cellar/ruby/1.9.2-p0/lib/ruby/gems
/1.9.1/gems/rails-2.3.8/lib/commands/server.rb:111
c:0006 p:---- s:0017 b:0017 l:000016 d:000016 FINISH
c:0005 p:---- s:0015 b:0015 l:000014 d:000014 CFUNC  :require
c:0004 p:0013 s:0011 b:0011 l:000010 d:000010 METHOD <internal:lib/rubygems/custom_require>:29
c:0003 p:0038 s:0006 b:0006 l:0015f8 d:000128 EVAL   ./script/server:3
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:0015f8 d:0015f8 TOP
---------------------------
-- Ruby level backtrace information ----------------------------------------
./script/server:3:in `<main>'
<internal:lib/rubygems/custom_require>:29:in `require'
<internal:lib/rubygems/custom_require>:29:in `require'
/usr/local/Cellar/ruby/1.9.2-p0/lib/ruby/gems/1.9.1/gems/rails-2.3.8/lib/commands/server.rb:111:in
 `<top (required)>'
/usr/local/Cellar/ruby/1.9.2-p0/lib/ruby/gems/1.9.1/gems/rack-1.1.0/lib/rack/handler/webrick.rb:14
:in `run'
/usr/local/Cellar/ruby/1.9.2-p0/lib/ruby/1.9.1/webrick/server.rb:81:in `start'
/usr/local/Cellar/ruby/1.9.2-p0/lib/ruby/1.9.1/webrick/server.rb:22:in `start'
/usr/local/Cellar/ruby/1.9.2-p0/lib/ruby/1.9.1/webrick/server.rb:90:in `block in start'
/usr/local/Cellar/ruby/1.9.2-p0/lib/ruby/1.9.1/webrick/server.rb:90:in `select'

-- C level backtrace information -------------------------------------------

[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

Abort trap
```

Related issues:

Related to Ruby master - Bug #3976: ruby/1.9.1/webrick/server.rb:90: [BUG] Se...	**Third Party's Issue**	**10/23/2010**
Related to Ruby master - Feature #3879: Segfault	**Closed**	**09/27/2010**
Has duplicate Ruby master - Bug #9730: E:/Rails/Ruby1.9.3/lib/ruby/1.9.1/web...	**Closed**	

History

#1 - 09/06/2010 08:41 AM - mrkn (Kenta Murata)

- Category set to lib

- Target version set to 1.9.2

- ruby -v set to ruby 1.9.2p0 (2010-08-18 revision 29036) [x86_64-darwin10.4.0]

Are there codes to reproduce this bug?

#2 - 09/09/2010 09:35 AM - naruse (Yui NARUSE)

- Status changed from Open to Feedback

#3 - 10/27/2010 06:59 PM - vjt (Marcello Barnaba)

Hello,

we've got a similar intermittent issue (circa 4/5 times a week, on a ~1000reqs/day site),
using Unicorn running under 1.9.1-p378 on a 64bit Linux kernel.

Crash report follows, I've also available a 160MB core dump and the ruby binary with
debug information. How should I make this data available to you?

Thanks!

~Marcello

```
/home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.4/lib/unicorn.rb:735: [BUG] Segmentation fault
ruby 1.9.1p378 (2010-01-10 revision 26273) [x86_64-linux]

-- control frame ----------
c:0018 p:---- s:0075 b:0075 l:000074 d:000074 CFUNC  :select
c:0017 p:0312 s:0068 b:0068 l:001cf8 d:001cf8 METHOD /home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.
4/lib/unicorn.rb:735
c:0016 p:0048 s:0057 b:0057 l:000038 d:000056 BLOCK  /home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.
4/lib/unicorn.rb:606
c:0015 p:---- s:0055 b:0055 l:000054 d:000054 FINISH
c:0014 p:---- s:0053 b:0053 l:000052 d:000052 CFUNC  :fork
c:0013 p:0104 s:0050 b:0048 l:000038 d:000047 BLOCK  /home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.
4/lib/unicorn.rb:603
c:0012 p:---- s:0044 b:0044 l:000043 d:000043 FINISH
c:0011 p:---- s:0042 b:0042 l:000041 d:000041 CFUNC  :each
c:0010 p:0023 s:0039 b:0039 l:000038 d:000038 METHOD /home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.
4/lib/unicorn.rb:599
c:0009 p:0060 s:0036 b:0036 l:000035 d:000035 METHOD /home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.
4/lib/unicorn.rb:613
c:0008 p:0345 s:0032 b:0032 l:000988 d:000988 METHOD /home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.
4/lib/unicorn.rb:270
c:0007 p:0031 s:0027 b:0027 l:000026 d:000026 METHOD /home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.
4/lib/unicorn.rb:29
c:0006 p:0346 s:0022 b:0022 l:000580 d:000580 TOP    /home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.
4/bin/unicorn_rails:210
c:0005 p:---- s:0013 b:0013 l:000012 d:000012 FINISH
c:0004 p:---- s:0011 b:0011 l:000010 d:000010 CFUNC  :load
c:0003 p:0127 s:0007 b:0007 l:001ec8 d:000230 EVAL   /home/panmind/.rvm/gems/ruby-1.9.1-p378/bin/unicorn_rails
:19
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:001ec8 d:001ec8 TOP
---------------------------
-- Ruby level backtrace information----------------------------------------
/home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.4/lib/unicorn.rb:735:in `select'
/home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.4/lib/unicorn.rb:735:in `worker_loop'
/home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.4/lib/unicorn.rb:606:in `block (2 levels) in spawn_mi
ssing_workers'
/home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.4/lib/unicorn.rb:603:in `fork'
/home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.4/lib/unicorn.rb:603:in `block in spawn_missing_worke
rs'
/home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.4/lib/unicorn.rb:599:in `each'
/home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.4/lib/unicorn.rb:599:in `spawn_missing_workers'
/home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.4/lib/unicorn.rb:613:in `maintain_worker_count'
/home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.4/lib/unicorn.rb:270:in `start'
/home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.4/lib/unicorn.rb:29:in `run'
```

```
/home/panmind/.rvm/gems/ruby-1.9.1-p378/gems/unicorn-1.1.4/bin/unicorn_rails:210:in `<top (required)>'
/home/panmind/.rvm/gems/ruby-1.9.1-p378/bin/unicorn_rails:19:in `load'
/home/panmind/.rvm/gems/ruby-1.9.1-p378/bin/unicorn_rails:19:in `<main>'

-- C level backtrace information -------------------------------------------
0x4e3ce1 unicorn_rails worker[12] -c config/unicorn.conf.rb -E production -D(rb_vm_bugreport+0x41) [0x4e3ce1]
0x510db8 unicorn_rails worker[12] -c config/unicorn.conf.rb -E production -D() [0x510db8]
0x510f21 unicorn_rails worker[12] -c config/unicorn.conf.rb -E production -D(rb_bug+0xb1) [0x510f21]
0x490d18 unicorn_rails worker[12] -c config/unicorn.conf.rb -E production -D() [0x490d18]
0x7f6133f858f0 /lib/libpthread.so.0(+0xf8f0) [0x7f6133f858f0]
0x479ae8 unicorn_rails worker[12] -c config/unicorn.conf.rb -E production -D() [0x479ae8]
0x479e59 unicorn_rails worker[12] -c config/unicorn.conf.rb -E production -D() [0x479e59]
0x7fff978884a0 [0x7fff978884a0]
```

#4 - 06/26/2011 03:22 PM - naruse (Yui NARUSE)

- Assignee set to kosaki (Motohiro KOSAKI)

#5 - 06/26/2011 03:27 PM - kosaki (Motohiro KOSAKI)

- Assignee changed from kosaki (Motohiro KOSAKI) to nahi (Hiroshi Nakamura)

#6 - 06/26/2011 04:02 PM - nahi (Hiroshi Nakamura)

- Target version changed from 1.9.2 to 1.9.3

#7 - 06/28/2011 12:42 PM - nahi (Hiroshi Nakamura)

- Subject changed from Seg fault in webrick to Seg fault in IO.select from webrick

#3879 looks similar to the original issue on OS X. SEGV from IO.select in WEBrick on ruby 1.9.2p0 (2010-08-18 revision 29036) [x86_64-darwin10.4.0].

#8 - 06/28/2011 12:44 PM - nahi (Hiroshi Nakamura)

Enrico, sorry for late reply.

Is it still occurs with the newer 1.9.2 version? (1.9.2p180 is the latest released version) Would you please try 1.9.2p180 or development version at trunk (if possible) and show us ~/Library/Logs/CrashReporter or /Library/Logs/CrashReporter for more investigation?

#9 - 06/28/2011 12:56 PM - nahi (Hiroshi Nakamura)

Marcello, sorry for late reply.

According to the dump you posted, though it threw SEGV at :select but it happened just after process forking by Unicorn. It must be a BUG of ruby but would you please consult with Unicorn devs first? They might have a similar issue report and effective workaround. And please file a new issue with crash logs on the latest ruby version.

#10 - 06/28/2011 01:53 PM - normalperson (Eric Wong)

Hiroshi Nakamura nakahiro@gmail.com wrote:

> Marcello, sorry for late reply.
>
> According to the dump you posted, though it threw SEGV at :select but it happened just after process forking by Unicorn. It must be a BUG of ruby but would you please consult with Unicorn devs first? They might have a similar issue report and effective workaround. And please file a new issue with crash logs on the latest ruby version.

(Unicorn BFDL speaking)

I just noticed this backtrace, but I have never encountered this with Unicorn. I even use x86_64-linux primarily and (at one point) had 1.9.1-p378 as my primary 1.9 install.

The only post-fork issue I remember from 1.9.1 is post-fork RNG reinitialization:

http://unicorn.bogomips.org/KNOWN_ISSUES.html
http://redmine.ruby-lang.org/issues/show/2962

--
Eric Wong

#11 - 07/09/2011 04:25 PM - ptressel (Pat Tressel)

- File Report.wer added

Hiroshi asked if the problem happens with a later version of Ruby -- it does. I am using 1.9.2p180 on Windows 7 64-bit. Ruby was installed using the installer from rubyinstaller.org. So now we have a full set -- it happens on Unix, Linux, and Windows.

Note this same crash was attributed to use of a debugger in another bug report -- I am not using a debugger. Also not using Unicorn. Not doing anything with SSL, Open or otherwise. Nor using PostgreSQL.

I'm attaching the Windows error report file, which mainly shows what libraries were loaded. I'm new to Ruby / Rails, so if "crash log" means something other than this, please tell me where it is and I'll provide it.

Thanks!

#12 - 10/07/2011 03:03 AM - briang@spiceworks.com (Brian Gugliemetti)

I am using 1.9.2-p290 on Windows XP and have seen this crash as well. The IO.select call is IO.select(nil, [socket], nil, 5). Uncertain if the timeout was hit. Here is the windbg backtrace (sorry, don't have the full symbols to include line numbers, but I'm hoping the trace with args helps track down):

```
ChildEBP RetAddr  Args to Child
0bb8ec30 7c8285e2 0bb8ed14 0bb8ffdc 0bb8ed30 kernel32!_except_handler3+0x61
0bb8ec54 7c8285b3 0bb8ed14 0bb8ffdc 0bb8ed30 ntdll!ExecuteHandler2+0x26
0bb8ecfc 7c8283ee 0bb86000 0bb8ed30 0bb8ed14 ntdll!ExecuteHandler+0x24
0bb8ecfc 10071320 0bb86000 0bb8ed30 0bb8ed14 ntdll!KiUserExceptionDispatcher+0xe
0bb8f008 10073d65 0000114c 0000114c 00000000 ruby_10000000!st_lookup+0x90
0bb8f01c 10073c30 0000114c 00000000 07b86d38 ruby_10000000!rb_w32_fdisset+0x1a5
0bb8f03c 100796e6 07b86d38 10073d50 0bb8f3cc ruby_10000000!rb_w32_fdisset+0x70
0bb8f3f8 10006379 00000016 00000000 07b86d38 ruby_10000000!rb_w32_select+0xe6
0bb8f780 1000713f 00000016 00000000 07b86d38 ruby_10000000!rb_thread_run+0x159
0bb8f79c 10024f93 00000016 00000000 0bb8f89c ruby_10000000!rb_thread_fd_select+0x6f
0bb8f7e4 1002539e 00000004 18e00c78 00000004 ruby_10000000!rb_io_stdio_file+0x723
0bb8f800 10001d09 0bb8f884 0bb8f8b4 0bb8f864 ruby_10000000!rb_io_stdio_file+0xb2e
0bb8f864 10025467 10025380 0bb8f884 100253b0 ruby_10000000!rb_ensure+0x49
0bb8f8c0 10035d9c 00000004 0b55018c 008065c4 ruby_10000000!rb_io_stdio_file+0xbf7
0bb8f8dc 10036134 100253e0 0083d2a8 0083d2e8 ruby_10000000!Init_Exception+0x66c
0bb8f8f0 1003b68b 00000004 008065c4 0083d2a8 ruby_10000000!Init_Exception+0xa04
0bb8f91c 1003c716 07d1c0f8 0b5cfcdc 00000000 ruby_10000000!rb_thread_alloc+0x71b
0bb8f990 1003e32e 07d1c0f8 07d1c0f8 0b5500d0 ruby_10000000!rb_thread_alloc+0x17a6
0bb8fa1c 1003ef00 07d1c0f8 0b5cfe3c 048dbd4c ruby_10000000!rb_vm_get_insns_address_table+0x44e
0bb8fa54 1003f340 07d1c0f8 048dbd4c 00000180 ruby_10000000!rb_vm_invoke_proc+0x250
0bb8fa84 10036291 048dbd4c 00000180 00000003 ruby_10000000!rb_call_super+0xd0
0bb8fad8 1003b839 07d1c0f8 048dbd4c 00000002 ruby_10000000!Init_Exception+0xb61
0bb8fb0c 1003c716 07d1c0f8 0b5cfe68 00000000 ruby_10000000!rb_thread_alloc+0x8c9
0bb8fb80 1003e32e 07d1c0f8 00000000 07d1c0f8 ruby_10000000!rb_thread_alloc+0x17a6
0bb8fc0c 1003ec70 07d1c0f8 08965ef0 07d1c0f8 ruby_10000000!rb_vm_get_insns_address_table+0x44e
0bb8fc28 1003ed24 08965ef0 07a82a58 00000001 ruby_10000000!rb_eval_string_wrap+0x240
0bb8fcac 1005512d 07d1c0f8 08965ef0 07a82a58 ruby_10000000!rb_vm_invoke_proc+0x74
0bb8fcd4 10035d9c 00000001 0b55003c 07a8279c ruby_10000000!rb_f_lambda+0x8d
0bb8fcf0 10036134 100550d0 00853650 00853670 ruby_10000000!Init_Exception+0x66c
0bb8fd04 1003b68b 00000001 07a8279c 00853650 ruby_10000000!Init_Exception+0xa04
0bb8fd30 1003c716 07d1c0f8 0b5cff9c 00000000 ruby_10000000!rb_thread_alloc+0x71b
0bb8fda4 1003e32e 07d1c0f8 00000000 07d1c0f8 ruby_10000000!rb_thread_alloc+0x17a6
0bb8fe30 1003ec70 07d1c0f8 08965f70 07d1c0f8 ruby_10000000!rb_vm_get_insns_address_table+0x44e
0bb8fe4c 1003ed24 08965f70 07a827d8 00000001 ruby_10000000!rb_eval_string_wrap+0x240
0bb8fed0 10006d3d 07d1c0f8 08965f70 07a827d8 ruby_10000000!rb_vm_invoke_proc+0x74
0bb8ff60 10007530 07d1c0f8 0bb8fffc 00000000 ruby_10000000!rb_thread_terminate_all+0x25d
0bb8ff74 78543433 00000538 c59a18d8 00000000 ruby_10000000!rb_barrier_wait+0x90
0bb8ffac 785434c7 00000000 0bb8ffec 77e6482f msvcr90!_endthreadex+0x44
0bb8ffb8 77e6482f 07a84010 00000000 00000000 msvcr90!_endthreadex+0xd8
0bb8ffec 00000000 7854345e 07a84010 00000000 kernel32!BaseThreadStart+0x34
```

The st_lookup method is passed 00000000 which is the root of the problem.

#13 - 12/10/2012 12:57 AM - mame (Yusuke Endoh)

- Target version changed from 1.9.3 to 2.0.0

Nahi-san, can you reproduce this issue?

--
Yusuke Endoh mame@tsg.ne.jp

#14 - 02/18/2013 09:15 PM - mame (Yusuke Endoh)

- Target version changed from 2.0.0 to 2.6

Nahi-san, can you reproduce this issue?

--
Yusuke Endoh mame@tsg.ne.jp

#15 - 05/27/2014 03:22 AM - nobu (Nobuyoshi Nakada)

- Has duplicate Bug #9730: E:/Rails/Ruby1.9.3/lib/ruby/1.9.1/webrick/server.rb:98: [BUG] Segmentation fault added

#16 - 05/27/2014 03:23 AM - nobu (Nobuyoshi Nakada)

- Description updated

#17 - 12/25/2017 06:14 PM - naruse (Yui NARUSE)

- Target version deleted (2.6)

#18 - 07/15/2019 07:27 PM - jeremyevans0 (Jeremy Evans)

- Status changed from Feedback to Closed

Files

Report.wer	13.6 KB	07/09/2011	ptressel (Pat Tressel)