Ruby trunk - Bug #15763

Segmentation fault in timeout.rb / sleep

04/11/2019 12:26 AM - stan-envato (Stan Pitucha)

Status:	Open		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.6.2p47 (2019-03-13 revision 67232) [x86_64-darwin18]	**Backport:**	2.4: UNKNOWN, 2.5: UNKNOWN, 2.6: UNKNOWN

Description

I'm running into crashes on both ruby 2.6.1 and 2.6.2 (2.5.x is all good).
I'm on OSX / mojave with ruby installed via rbenv / ruby-build. Confirmed on two different machines.

The crash happens through the parallel gem, but it happens even if the number of processes is reduced to 1.

Short summary:

-- Control frame information --
c:0003 p:---- s:0011 e:000010 CFUNC :sleep
c:0002 p:0025 s:0006 e:000005 BLOCK /Users/viraptor/.rbenv/versions/2.6.2/lib/ruby/2.6.0/timeout.rb:86 [FINISH]
c:0001 p:---- s:0003 e:000002 (none) [FINISH]

-- Ruby level backtrace information --
/Users/viraptor/.rbenv/versions/2.6.2/lib/ruby/2.6.0/timeout.rb:86:in block (2 levels) in timeout'
/Users/viraptor/.rbenv/versions/2.6.2/lib/ruby/2.6.0/timeout.rb:86:insleep'

The rest is in the logs.

History

#1 - 04/11/2019 01:37 AM - stan-envato (Stan Pitucha)

Additionally, the issue does not seem to happen on every build. If I rebuild the same version of ruby, the issue may go away. (until another few rebuilds)

#2 - 04/11/2019 05:11 AM - mame (Yusuke Endoh)

This might be the same issue as:

- https://bugs.ruby-lang.org/issues/15490
- https://bugs.ruby-lang.org/issues/15639
- https://github.com/hanami/hanami/issues/993

The common points are:

- macOS (darwin17 or 18)
- uses multiple threads
- segfault in getaddrinfo

I could be wrong, but I suspect a bug of macOS's getaddrinfo.

Can you show a short program that causes the segfault?

#3 - 05/18/2019 12:17 AM - alexagranov (Alex Agranov)

I came here after seeing the same segfault in timeout.rb / CFUNC :sleep on ruby 2.6.2 on MacOS with a Rails project running with Puma and 2 worker threads.

Installed 2.6.3 and now seeing the segfault coming from pg - but interestingly while opening a connection to the db:

```
-- C level backtrace information -------------------------------------------
/Users/agranov/.rvm/rubies/ruby-2.6.3/lib/libruby.2.6.dylib(rb_vm_bugreport+0x82) [0x10bd87182]
/Users/agranov/.rvm/rubies/ruby-2.6.3/lib/libruby.2.6.dylib(rb_bug_context+0x1d3) [0x10bbd31f3]
/Users/agranov/.rvm/rubies/ruby-2.6.3/lib/libruby.2.6.dylib(sigsegv+0x51) [0x10bceb591]
/usr/lib/system/libsystem_platform.dylib(_sigtramp+0x1d) [0x7fff5827db5d]
/usr/lib/system/libsystem_trace.dylib(_os_log_preferences_refresh+0x4c) [0x7fff582a090a]
```

```
/usr/lib/system/libsystem_trace.dylib(0x7fff582a113d) [0x7fff582a113d]
/usr/lib/system/libsystem_info.dylib(si_destination_compare_statistics+0x903) [0x7fff581b9843]
/usr/lib/system/libsystem_info.dylib(0x7fff581b81a5) [0x7fff581b81a5]
/usr/lib/system/libsystem_info.dylib(0x7fff581b7d3f) [0x7fff581b7d3f]
/usr/lib/system/libsystem_info.dylib(0x7fff581966df) [0x7fff581966df]
/usr/lib/system/libsystem_c.dylib(_isort+0xc1) [0x7fff58140e5b]
/usr/lib/system/libsystem_c.dylib(0x7fff58140d88) [0x7fff58140d88]
/usr/lib/system/libsystem_info.dylib(0x7fff5818df2d) [0x7fff5818df2d]
/usr/lib/system/libsystem_info.dylib(0x7fff5818c885) [0x7fff5818c885]
/usr/lib/system/libsystem_info.dylib(0x7fff5818bf77) [0x7fff5818bf77]
/usr/lib/system/libsystem_info.dylib(0x7fff5818be7d) [0x7fff5818be7d]
/usr/lib/libpq.5.dylib(connectDBStart+0x1d4) [0x7fff57094af2]
/usr/lib/libpq.5.dylib(PQconnectStart+0x3a) [0x7fff570941de]
/usr/lib/libpq.5.dylib(PQconnectdb+0xb) [0x7fff57094181]
```

Reducing the Puma workers to a single one, I've yet to see a segfault.

#4 - 05/18/2019 01:04 AM - alexagranov (Alex Agranov)

Nix that: single Puma worker makes no difference. Back to segfault in timeout.rb.

Files

crash_log	68.9 KB	04/11/2019	stan-envato (Stan Pitucha)
ruby_2019-04-11-101832-3_Stans-MacBook-Pro.crash	44.7 KB	04/11/2019	stan-envato (Stan Pitucha)