Ruby - Bug #12308

segfault in add_signal_thread_list

04/22/2016 02:31 AM - ice799 (Joe Damato)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:		**Backport:**	2.1: WONTFIX, 2.2: REQUIRED, 2.3: DONTNEED

Description

Greetings:

On very rare occasions, my Ruby 2.1.9 segfaults when calling malloc from add_signal_thread_list with the following stack trace:

```
#21 0x00007f9f0f0f129a in add_signal_thread_list (th=0x7f9f110c4000) at thread_pthread.c:1111
#22 0x00007f9f0f0f1437 in ubf_select (ptr=0x7f9f110c4000) at thread_pthread.c:1166
#23 0x00007f9f0f0f1e2c in rb_threadptr_interrupt_common (th=0x7f9f110c4000, trap=1) at thread.c:34
9
#24 0x00007f9f0f0f1e8e in rb_threadptr_trap_interrupt (th=0x7f9f110c4000) at thread.c:367
#25 0x00007f9f0f0f7112 in rb_threadptr_check_signal (mth=0x7f9f110c4000) at thread.c:3820
#26 0x00007f9f0f0f718a in timer_thread_function (arg=0x0) at thread.c:3841
#27 0x00007f9f0f0f1893 in thread_timer (p=0x7f9f110c0008) at thread_pthread.c:1449
#28 0x00007f9f0eb3ee9a in start_thread (arg=0x7f9f0ef71700) at pthread_create.c:308
```

I believe this is due to the Ruby VM being in an async-unsafe state when malloc is called here:

```
static void
add_signal_thread_list(rb_thread_t *th)
{
    if (!th->native_thread_data.signal_thread_list) {
        FGLOCK(&signal_thread_list_lock, {
            struct signal_thread_list *list =
              malloc(sizeof(struct signal_thread_list));
```

This code is also present in Ruby 2.2.x.

This commit https://github.com/ruby/ruby/commit/487748fac8b43936bca1209c22fcd995a739aa93 removes the call to malloc in Ruby 2.3.x as part of a larger refactor.

I backported the commit above to my Ruby 2.1.9 and have been running it for over 1-month in production with no segfaults. I have included my very sloppy backported patch to this bug report.

I know that this patch will be unacceptable for several reasons:

1. It is a very sloppy backport
2. No new code is going into Ruby 2.1.x
3. Other reasons

Hopefully this patch and bug report will be useful to people hitting this segfault on Ruby 2.2.x.

History

#1 - 04/28/2016 05:13 AM - naruse (Yui NARUSE)

- Status changed from Open to Closed

- Backport changed from 2.1: UNKNOWN, 2.2: UNKNOWN, 2.3: UNKNOWN to 2.1: WONTFIX, 2.2: REQUIRED, 2.3: DONTNEED

Change state to "Closed" to enqueue backporitng process.

Files

remove_malloc_from_signal_list.patch	40.8 KB	04/22/2016	ice799 (Joe Damato)