Ruby - Bug #12290

Possible segfault with Thread#name=

04/15/2016 11:07 AM - herwinw (Herwin Quarantainenet)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.3.0p0 (2015-12-25 revision 53290)	**Backport:**	2.1: DONTNEED, 2.2: DONTNEED, 2.3: DONE

Description

Ruby 2.3 added a Thread#name=, which may segfault when used incorrectly. This little program:

```
class SubClassedThread < Thread
  def initialize()
    self.name = 'foo'
    super do
      yield
    end
  end
end

SubClassedThread.new {}
```

Causes a segfault with both Ruby 2.3 (ruby 2.3.0p0 (2015-12-25 revision 53290)) and ruby-2.4.0-dev (ruby 2.4.0dev (2016-04-15 trunk 54594)). Moving the line that assignes the name in the block passed to super resolves the issue. Even thought there is a workaround, it shouldn't be possible to trigger a segfault from a script imho.

The relevant lines of the backtrace

```
/lib/i386-linux-gnu/i686/cmov/libpthread.so.0(pthread_setname_np+0x50) [0xf739ded0]
ruby(rb_thread_setname+0x95) [0xf755dc85] thread.c:2797
```

The system is a default Debian Jessie (32bit), with libc version 2.19-18+deb8u4.

Associated revisions

Revision f7d0059e3643ad1713b8abe4969147e2bc185d75 - 04/15/2016 12:12 PM - nobu (Nobuyoshi Nakada)

thread.c: must be initialized to set name

- thread.c (get_initialized_threadptr): extract ensuring that the thread is initialized.
- thread.c (rb_thread_setname): thread must be initialized to set the name. [ruby-core:74963] [Bug #12290]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@54598 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision f7d0059e - 04/15/2016 12:12 PM - nobu (Nobuyoshi Nakada)

thread.c: must be initialized to set name

- thread.c (get_initialized_threadptr): extract ensuring that the thread is initialized.
- thread.c (rb_thread_setname): thread must be initialized to set the name. [ruby-core:74963] [Bug #12290]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@54598 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 4bf8fa83b7084040fbe12cc003f881ccf128c911 - 04/15/2016 01:30 PM - nobu (Nobuyoshi Nakada)

thread.c: defer setting name in initialize

- thread.c (rb_thread_setname): defer setting native thread name set in initialize until the native thread is created. [ruby-core:74963] [Bug #12290]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@54600 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 4bf8fa83 - 04/15/2016 01:30 PM - nobu (Nobuyoshi Nakada)

thread.c: defer setting name in initialize

- thread.c (rb_thread_setname): defer setting native thread name
  set in initialize until the native thread is created.
  [ruby-core:74963] [Bug #12290]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@54600 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 260d1ac2ca8711971c48e14bd535aeeb20f6ed1d - 04/15/2016 04:07 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 54598,54600: [Backport #12290]

```
    * thread.c (get_initialized_threadptr): extract ensuring that the
      thread is initialized.

    * thread.c (rb_thread_setname): thread must be initialized to set
      the name.  [ruby-core:74963] [Bug #12290]

    * thread.c (rb_thread_setname): defer setting native thread name
      set in initialize until the native thread is created.
      [ruby-core:74963] [Bug #12290]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@54607 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 260d1ac2 - 04/15/2016 04:07 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 54598,54600: [Backport #12290]

```
    * thread.c (get_initialized_threadptr): extract ensuring that the
      thread is initialized.

    * thread.c (rb_thread_setname): thread must be initialized to set
      the name.  [ruby-core:74963] [Bug #12290]

    * thread.c (rb_thread_setname): defer setting native thread name
      set in initialize until the native thread is created.
      [ruby-core:74963] [Bug #12290]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@54607 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 04/15/2016 11:14 AM - herwinw (Herwin Quarantainenet)

And of course the backtrace can be improved when installing the debugging symbols for libc

```
/lib/i386-linux-gnu/i686/cmov/libpthread.so.0(pthread_setname_np+0x50) [0xf73e0ed0] ../nptl/sysdeps/unix/sysv/
linux/pthread_setname.c:49
```

The exact source can be downloaded from https://packages.debian.org/jessie/libc6 (keep in mind that the original source and the packages have to be downloaded separately, and be combined.

#2 - 04/15/2016 11:23 AM - herwinw (Herwin Quarantainenet)

And since it's pretty easy to get the relevant source on a running debian system:

```
int
pthread_setname_np (th, name)
     pthread_t th;
     const char *name;
{
  const struct pthread *pd = (const struct pthread *) th;
...
#define FMT "/proc/self/task/%u/comm"
  char fname[sizeof (FMT) + 8];
  sprintf (fname, FMT, (unsigned int) pd->tid);
```

Line 49 is the last line, and this is indeed the first part where a member of td is queried.

#3 - 04/15/2016 11:44 AM - herwinw (Herwin Quarantainenet)

- File issue12290_segthread_thread_name.diff added

And this is the simplest solution I could think of. It throws an exception, which is a better way to react than a segfault. Making it actually work would of course be even better.

#4 - 04/15/2016 11:51 AM - herwinw (Herwin Quarantainenet)

- File issue12290_segthread_thread_name.diff added

That patch still segfaulted when using self.name = nil. Version 2 attached.

#5 - 04/15/2016 12:12 PM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

Applied in changeset r54598.

---

thread.c: must be initialized to set name

- thread.c (get_initialized_threadptr): extract ensuring that the thread is initialized.
- thread.c (rb_thread_setname): thread must be initialized to set the name. [ruby-core:74963] [Bug #12290]

#6 - 04/15/2016 01:36 PM - nobu (Nobuyoshi Nakada)

- Description updated

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

#7 - 04/15/2016 04:07 PM - nagachika (Tomoyuki Chikanaga)

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

ruby_2_3 r54607 merged revision(s) 54598,54600.

Files

issue12290_segthread_thread_name.diff	486 Bytes	04/15/2016	herwinw (Herwin Quarantainenet)
issue12290_segthread_thread_name.diff	393 Bytes	04/15/2016	herwinw (Herwin Quarantainenet)