# Backport192 - Backport #4367

## Thread.kill segfaults when the object to be killed isn't a thread

02/04/2011 10:43 PM - agrimm (Andrew Grimm)

| | | |
|---|---|---|
| **Status:** | Closed | |
| **Priority:** | Normal | |
| **Assignee:** | yugui (Yuki Sonoda) | |

**Description**

=begin
If something other than a thread is supplied to Thread.kill, a segfault occurs. For example, Thread.kill(nil) causes a segfault:

Andrew-Grimms-MacBook-Pro:~ agrimm$ ruby
Thread.kill(nil)
-:1: [BUG] Segmentation fault
ruby 1.9.3dev (2011-01-29 trunk 30720) [x86_64-darwin10.4.0]

-- Control frame information -----------------------------------------------
c:0004 p:---- s:0010 b:0010 l:000009 d:000009 CFUNC  :kill
c:0003 p:0016 s:0006 b:0006 l:002358 d:000798 EVAL   -:1
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:002358 d:002358 TOP

-- Ruby level backtrace information ----------------------------------------
-:1:in <main>'
-:1:inkill'

-- See Crash Report log file under ~/Library/Logs/CrashReporter or ---------
-- /Library/Logs/CrashReporter, for the more detail of ----------------------
-- C level backtrace information -------------------------------------------

-- Other runtime information -----------------------------------------------

- Loaded script: -

- Loaded features:

  0 enumerator.so
  1 /Users/agrimm/.rvm/rubies/ruby-head/lib/ruby/1.9.1/x86_64-darwin10.4.0/enc/encdb.bundle
  2 /Users/agrimm/.rvm/rubies/ruby-head/lib/ruby/1.9.1/x86_64-darwin10.4.0/enc/trans/transdb.bundle
  3 /Users/agrimm/.rvm/rubies/ruby-head/lib/ruby/1.9.1/rubygems/defaults.rb
  4 /Users/agrimm/.rvm/rubies/ruby-head/lib/ruby/1.9.1/x86_64-darwin10.4.0/rbconfig.rb
  5 /Users/agrimm/.rvm/rubies/ruby-head/lib/ruby/1.9.1/thread.rb
  6 /Users/agrimm/.rvm/rubies/ruby-head/lib/ruby/1.9.1/rubygems/exceptions.rb
  7 /Users/agrimm/.rvm/rubies/ruby-head/lib/ruby/1.9.1/rubygems/custom_require.rb
  8 /Users/agrimm/.rvm/rubies/ruby-head/lib/ruby/1.9.1/rubygems.rb

[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
=end

### Associated revisions

**Revision 3202eea1 - 05/01/2011 09:37 AM - yugui (Yuki Sonoda)**

- thread.c (thread_s_kill): workaround for [ruby-core:35086].
  fixes #4367.

- test/ruby/test_thread.rb (TestThread#test_kill_wrong_argument):
  test for [ruby-core:35086].

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_2@31402 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

**Revision 31402 - 05/01/2011 09:37 AM - yugui (Yuki Sonoda)**

- thread.c (thread_s_kill): workaround for [ruby-core:35086].
  fixes #4367.

- test/ruby/test_thread.rb (TestThread#test_kill_wrong_argument):
  test for [ruby-core:35086].

## History

**#1 - 02/05/2011 01:03 AM - kosaki (Motohiro KOSAKI)**

=begin
2011/2/4 Andrew Grimm redmine@ruby-lang.org:

> Bug #4367: Thread.kill segfaults when the object to be killed isn't a thread
> http://redmine.ruby-lang.org/issues/show/4367
>
> Author: Andrew Grimm
> Status: Open, Priority: Normal
> ruby -v: ruby 1.9.3dev (2011-01-29 trunk 30720) [x86_64-darwin10.4.0]
>
> If something other than a thread is supplied to Thread.kill, a segfault occurs. For example, Thread.kill(nil) causes a segfault:
>
> Andrew-Grimms-MacBook-Pro:~ agrimm$ ruby
> Thread.kill(nil)
> -:1: [BUG] Segmentation fault
> ruby 1.9.3dev (2011-01-29 trunk 30720) [x86_64-darwin10.4.0]

Good catch!

Yes, current GetThreadPtr has no type check and can makes bad cast.
I'll fix it soon.

=end

**#2 - 02/05/2011 01:07 AM - kosaki (Motohiro KOSAKI)**

*- Status changed from Open to Closed*

*- % Done changed from 0 to 100*

=begin
This issue was solved with changeset r30781.
Andrew, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

---

- vm_core.h (GetThreadPtr): use TypedData_Get_Struct() instead
  CoreDataFromValue() because we need type check. Otherwise,
  type mismatch can cause segmentation fault crash.
  [ruby-core:35086] [Ruby 1.9-Bug#4367]

  - vm.c (thread_data_type): remove static. =end

**#3 - 02/05/2011 01:08 AM - kosaki (Motohiro KOSAKI)**

*- Category set to core*

*- Status changed from Closed to Assigned*

*- Assignee set to yugui (Yuki Sonoda)*

*- Target version set to 1.9.2*

=begin
I bet this need to be backported.
=end

#### #4 - 02/06/2011 11:19 AM - nobu (Nobuyoshi Nakada)

*- Category set to core*

=begin

=end

#### #5 - 05/01/2011 06:37 PM - yugui (Yuki Sonoda)

*- Status changed from Assigned to Closed*

This issue was solved with changeset r31402.
Andrew, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

---

- thread.c (thread_s_kill): workaround for [ruby-core:35086].
  fixes #4367.

- test/ruby/test_thread.rb (TestThread#test_kill_wrong_argument):
  test for [ruby-core:35086].

#### #6 - 06/09/2011 11:19 PM - nagachika (Tomoyuki Chikanaga)

Hi,

I found by change current 1.9.2-head raise TypeError like below.

```
class T < Thread
end
t = T.new { sleep }
Thread.kill(t)  #=> TypeError
```

I attach a patch for it.
And test for it was commited by r31967 in trunk. Please backport that.

Regard,

#### #7 - 06/09/2011 11:21 PM - nagachika (Tomoyuki Chikanaga)

*- File thread_kill_subclass.patch added*

Sorry, I forgot to attach the patch. here it is.

### Files

| | | | |
|---|---|---|---|
| ruby_2011-02-05-003336_Andrew-Grimms-MacBook-Pro.crash | 4.29 KB | 02/04/2011 | agrimm (Andrew Grimm) |
| thread_kill_subclass.patch | 451 Bytes | 06/09/2011 | nagachika (Tomoyuki Chikanaga) |