Ruby trunk - Bug #6400

dl/callback with fiddle occurs SEGV on NetBSD amd64

05/04/2012 09:33 PM - naruse (Yui NARUSE)

Status:	Assigned		
Priority:	Normal		
Assignee:	tenderlovemaking (Aaron Patterson)		
Target version:			
ruby -v:	ruby 2.0.0dev (2012-04-30 trunk 35500) [x86_64-netbsd6.99.5]	**Backport:**	

Description

On NetBSD amd64, libffi with callback occurs SEGV as following.

```
kelvena%  cat p
require 'dl/callback'
require 'dl/func'
include DL
Called_with = nil
addr = set_callback(TYPE_VOID, 1) do |str|
called_with = dlunwrap(str)
end
func = CFunc.new(addr, TYPE_VOID, 'test')
f = Function.new(func, [TYPE_VOIDP])
arg = 'foo'
f.call(dlwrap(arg))
kelvena% ./ruby p
/home/naruse/local/ruby/lib/ruby/2.0.0/dl/func.rb:55: [BUG] Segmentation fault
ruby 2.0.0dev (2012-04-30 trunk 35500) [x86_64-netbsd6.99.5]

-- Control frame information -----------------------------------------------
c:0005 p:---- s:0022 b:0022 l:000021 d:000021 CFUNC  :call
c:0004 p:0059 s:0018 b:0018 l:000017 d:000017 METHOD /home/naruse/local/ruby/lib/ruby/2.0.0/dl/func.
rb:55
c:0003 p:0157 s:0010 b:0010 l:001db8 d:0021a8 EVAL   p:11
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:001db8 d:001db8 TOP

-- Ruby level backtrace information ----------------------------------------
p:11:in <main>'
/home/naruse/local/ruby/lib/ruby/2.0.0/dl/func.rb:55:incall'
/home/naruse/local/ruby/lib/ruby/2.0.0/dl/func.rb:55:in `call'

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

- Loaded script: p
- Loaded features:

  0 enumerator.so
  1 /home/naruse/local/ruby/lib/ruby/2.0.0/x86_64-netbsd6.99.5/enc/encdb.so
  2 /home/naruse/local/ruby/lib/ruby/2.0.0/x86_64-netbsd6.99.5/enc/trans/transdb.so
  3 /home/naruse/local/ruby/lib/ruby/2.0.0/rubygems/defaults.rb
  4 /home/naruse/local/ruby/lib/ruby/2.0.0/x86_64-netbsd6.99.5/rbconfig.rb
  5 /home/naruse/local/ruby/lib/ruby/2.0.0/rubygems/deprecate.rb
  6 /home/naruse/local/ruby/lib/ruby/2.0.0/rubygems/exceptions.rb
  7 /home/naruse/local/ruby/lib/ruby/2.0.0/rubygems/custom_require.rb
  8 /home/naruse/local/ruby/lib/ruby/2.0.0/rubygems.rb
  9 /home/naruse/local/ruby/lib/ruby/2.0.0/x86_64-netbsd6.99.5/dl.so
  10 /home/naruse/local/ruby/lib/ruby/2.0.0/x86_64-netbsd6.99.5/fiddle.so
  11 /home/naruse/local/ruby/lib/ruby/2.0.0/fiddle/function.rb
  12 /home/naruse/local/ruby/lib/ruby/2.0.0/fiddle/closure.rb
  13 /home/naruse/local/ruby/lib/ruby/2.0.0/fiddle.rb

```
14 /home/naruse/local/ruby/lib/ruby/2.0.0/dl.rb
15 /home/naruse/local/ruby/lib/ruby/2.0.0/thread.rb
16 /home/naruse/local/ruby/lib/ruby/2.0.0/dl/callback.rb
17 /home/naruse/local/ruby/lib/ruby/2.0.0/dl/stack.rb
18 /home/naruse/local/ruby/lib/ruby/2.0.0/dl/value.rb
19 /home/naruse/local/ruby/lib/ruby/2.0.0/dl/func.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

zsh: abort (core dumped)  ./ruby p
```

History

#1 - 05/04/2012 11:10 PM - naruse (Yui NARUSE)

- Description updated

#2 - 08/15/2013 05:06 AM - zzak (Zachary Scott)

Is this related to #6592?