

## Ruby trunk - Bug #4162

### C segfault in TCPSocket CFUNC :read

12/15/2010 08:43 PM - EnabrenTane (Chris Lundquist)

<b>Status:</b> Closed	
<b>Priority:</b> Normal	
<b>Assignee:</b>	
<b>Target version:</b>	
<b>ruby -v:</b> ruby 1.9.2p0 (2010-08-18 revision 29036) [x86_64-linux]	<b>Backport:</b>

**Description**

=begin  
Please let me know how I can be of assistance. The errors below are reproducible and consistent for me.

Code can be found here:  
<https://github.com/ChrisLundquist/Handbrake-Network-Queue/tree/88c4ed38be1a871dfd5d012594710ea3dc0bb02c>

This is a bug specific to 1.9 as the same code behaves as desired on 1.8.7

Obviously I cannot attach large copy righted files, but I would suspect you would encounter this errors with other similar large binary files.

I also get this error with a different file. It may be related.  
NOTE: the below error happens 4mb into the file after it has already transferred 1.4GB of previous files.  
wrong argument type Object (expected Data)  
Occurs when transferring VTS\_01\_2.VOB of GLADIATOR

Attached is the last thing it reads from the socket before attempting to write it to the file.

I encounter the below error when transferring VTS\_01\_1.VOB of GLADIATOR

This only seems to happen with binary data files.

```
/home/clundquist/code/ruby/Handbrake-Network-Queue/ruby/lib/file_transfer.rb:71: [BUG] Segmentation fault
ruby 1.9.2p0 (2010-08-18 revision 29036) [x86_64-linux]

-- control frame -----
c:0013 p:---- s:0044 b:0044 l:000043 d:000043 CFUNC :read
c:0012 p:0014 s:0040 b:0040 l:000032 d:000039 BLOCK
/home/clundquist/code/ruby/Handbrake-Network-Queue/ruby/lib/file_transfer.rb:71
c:0011 p:---- s:0038 b:0038 l:000037 d:000037 FINISH
c:0010 p:---- s:0036 b:0036 l:000035 d:000035 CFUNC :times
c:0009 p:0227 s:0033 b:0033 l:000032 d:000032 METHOD
/home/clundquist/code/ruby/Handbrake-Network-Queue/ruby/lib/file_transfer.rb:69
c:0008 p:0018 s:0023 b:0023 l:000014 d:000022 BLOCK
/home/clundquist/code/ruby/Handbrake-Network-Queue/ruby/lib/client.rb:68
c:0007 p:---- s:0020 b:0020 l:000019 d:000019 FINISH
c:0006 p:---- s:0018 b:0018 l:000017 d:000017 CFUNC :times
c:0005 p:0107 s:0015 b:0015 l:000014 d:000014 METHOD
/home/clundquist/code/ruby/Handbrake-Network-Queue/ruby/lib/client.rb:67
c:0004 p:0019 s:0011 b:0011 l:000010 d:000010 METHOD
/home/clundquist/code/ruby/Handbrake-Network-Queue/ruby/lib/client.rb:24
c:0003 p:0095 s:0008 b:0008 l:0010e8 d:001cf8 EVAL ./client.rb:9
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:0010e8 d:0010e8 TOP
```

-- Ruby level backtrace information -----  
./client.rb:9:in <main>  
/home/clundquist/code/ruby/Handbrake-Network-Queue/ruby/lib/client.rb:24:inrun'  
/home/clundquist/code/ruby/Handbrake-Network-Queue/ruby/lib/client.rb:67:in checkout\_job'  
/home/clundquist/code/ruby/Handbrake-Network-Queue/ruby/lib/client.rb:67:in times'

```
/home/clundquist/code/ruby/Handbrake-Network-Queue/ruby/lib/client.rb:68:in block in checkout_job'  
/home/clundquist/code/ruby/Handbrake-Network-Queue/ruby/lib/file_transfer.rb:69:in recv'  
/home/clundquist/code/ruby/Handbrake-Network-Queue/ruby/lib/file_transfer.rb:69:in times'  
/home/clundquist/code/ruby/Handbrake-Network-Queue/ruby/lib/file_transfer.rb:71:in block in recv'  
/home/clundquist/code/ruby/Handbrake-Network-Queue/ruby/lib/file_transfer.rb:71:in `read'
```

```
-- C level backtrace information -----  
/usr/lib/libruby-1.9.1.so.1.9(rb_vm_bugreport+0x5f) [0x7fe240a67e8f]  
/usr/lib/libruby-1.9.1.so.1.9(+0x58a56) [0x7fe240972a56]  
/usr/lib/libruby-1.9.1.so.1.9(rb_bug+0xb3) [0x7fe240972bc3]  
/usr/lib/libruby-1.9.1.so.1.9(+0xedde5) [0x7fe240a07de5]  
/lib/libpthread.so.0(+0xfb40) [0x7fe24070cb40]  
/usr/lib/libruby-1.9.1.so.1.9(st_lookup+0x88) [0x7fe240a0ec58]  
/usr/lib/libruby-1.9.1.so.1.9(+0x124b8f) [0x7fe240a3eb8f]  
/usr/lib/libruby-1.9.1.so.1.9(rb_class_path+0x16) [0x7fe240a3ef66]  
/usr/lib/libruby-1.9.1.so.1.9(rb_class2name+0x9) [0x7fe240a3f0e9]  
/usr/lib/libruby-1.9.1.so.1.9(rb_check_type+0xf6) [0x7fe240974016]  
/usr/lib/libruby-1.9.1.so.1.9(rb_check_typeddata+0x30) [0x7fe240974130]  
/usr/lib/libruby-1.9.1.so.1.9(rb_mutex_trylock+0x22) [0x7fe240a69902]  
/usr/lib/libruby-1.9.1.so.1.9(rb_mutex_lock+0x16) [0x7fe240a6bfa6]  
/usr/lib/libruby-1.9.1.so.1.9(rb_mutex_synchronize+0x21) [0x7fe240a6c381]  
/usr/lib/libruby-1.9.1.so.1.9(+0x74c17) [0x7fe24098ec17]  
/usr/lib/libruby-1.9.1.so.1.9(+0x7c470) [0x7fe240996470]  
/usr/lib/libruby-1.9.1.so.1.9(rb_io_fptr_finalize+0x25) [0x7fe2409965a5]  
/usr/lib/libruby-1.9.1.so.1.9(+0x6b1dc) [0x7fe2409851dc]  
/usr/lib/libruby-1.9.1.so.1.9(+0x6b27a) [0x7fe24098527a]  
/usr/lib/libruby-1.9.1.so.1.9(+0x151615) [0x7fe240a6b615]  
/usr/lib/libruby-1.9.1.so.1.9(+0x1518ea) [0x7fe240a6b8ea]  
/usr/lib/libruby-1.9.1.so.1.9(rb_thread_blocking_region+0x59) [0x7fe240a6e129]  
/usr/lib/libruby-1.9.1.so.1.9(+0x75bc1) [0x7fe24098fbc1]  
/usr/lib/libruby-1.9.1.so.1.9(+0x7a0e8) [0x7fe2409940e8]  
/usr/lib/libruby-1.9.1.so.1.9(+0x147258) [0x7fe240a61258]  
/usr/lib/libruby-1.9.1.so.1.9(+0x13f410) [0x7fe240a59410]  
/usr/lib/libruby-1.9.1.so.1.9(+0x143e31) [0x7fe240a5de31]  
/usr/lib/libruby-1.9.1.so.1.9(rb_yield+0x238) [0x7fe240a663a8]  
/usr/lib/libruby-1.9.1.so.1.9(+0x935b1) [0x7fe2409ad5b1]  
/usr/lib/libruby-1.9.1.so.1.9(+0x147258) [0x7fe240a61258]  
/usr/lib/libruby-1.9.1.so.1.9(+0x13f410) [0x7fe240a59410]  
/usr/lib/libruby-1.9.1.so.1.9(+0x143e31) [0x7fe240a5de31]  
/usr/lib/libruby-1.9.1.so.1.9(rb_yield+0x238) [0x7fe240a663a8]  
/usr/lib/libruby-1.9.1.so.1.9(+0x935b1) [0x7fe2409ad5b1]  
/usr/lib/libruby-1.9.1.so.1.9(+0x147258) [0x7fe240a61258]  
/usr/lib/libruby-1.9.1.so.1.9(+0x13f410) [0x7fe240a59410]  
/usr/lib/libruby-1.9.1.so.1.9(+0x143e31) [0x7fe240a5de31]  
/usr/lib/libruby-1.9.1.so.1.9(rb_iseq_eval_main+0xb2) [0x7fe240a5e082]  
/usr/lib/libruby-1.9.1.so.1.9(+0x5bd52) [0x7fe240975d52]  
/usr/lib/libruby-1.9.1.so.1.9(ruby_exec_node+0x1d) [0x7fe240975d7d]  
/usr/lib/libruby-1.9.1.so.1.9(ruby_run_node+0x1e) [0x7fe24097763e]  
ruby(main+0x4b) [0x40092b]  
/lib/libc.so.6(__libc_start_main+0xfe) [0x7fe23fad0d8e]  
ruby() [0x400819]  
=end
```

#### Related issues:

Is duplicate of Backport192 - Backport #3910: SEGV at fptr\_finalize

Closed

10/06/2010

#### History

##### #1 - 12/15/2010 09:46 PM - EnabrenTane (Chris Lundquist)

=begin

Out of curiosity I checked out and compiled the svn 1.9.2 branch.

All of my issues are resolved in the below version of ruby.  
ruby 1.9.2p94 (2010-12-08 revision 30140) [x86\_64-linux]

I commend you all on a job well done.

I look forward to the official release (and the update on the Ubuntu package) of 1.9.2p94

=end

**#2 - 12/15/2010 09:53 PM - nobu (Nobuyoshi Nakada)**

*- Status changed from Open to Closed*

=begin

=end

**Files**

---

bug.report	11.4 KB	12/15/2010	EnabrenTane (Chris Lundquist)
------------	---------	------------	-------------------------------