

Ruby - Bug #8320

Ruby interpreter crashes when running pcaprub

04/24/2013 09:35 PM - crondaemon (Dario Lombardo)

Status:	Third Party's Issue	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 2.0.0dev (2012-11-01 trunk 37411) [i686-linux]	Backport: 1.9.3: UNKNOWN, 2.0.0: UNKNOWN

Description

Here's the code (taken from examples) that caused the crash:

```
require 'rubygems'
require 'pcaprub'

capture = PCAPRUB::Pcap.open_live('eth0', 65535, true, 0)
capture.setfilter('icmp')
capture.each do |packet|
  puts capture.dump(packet.length, packet.length, packet)
end
```

The code was run with

```
gem install pcaprub
rvmsudo ruby testpcaprub.rb
```

Ruby was installed with rvm. Code causes crash with:

```
ruby 2.0.0dev (2012-11-01 trunk 37411) [i686-linux]
ruby 1.9.3p286 (2012-10-12 revision 37165) [i686-linux]
ruby 1.8.7 (2012-10-12 patchlevel 371) [i686-linux]
```

The expected behavior from the code was to print the captured packets (don't know exactly how, since this was my first test).

Crash dump:

```
$ rvmsudo ruby testpcaprub.rb
testpcaprub.rb:10: [BUG] Segmentation fault
ruby 2.0.0dev (2012-11-01 trunk 37411) [i686-linux]

-- Control frame information -----
c:0005 p:---- s:0018 e:000017 CFUNC :dump
c:0004 p:0021 s:0012 e:000010 BLOCK testpcaprub.rb:10 [FINISH]
c:0003 p:---- s:0008 e:000007 CFUNC :<>
c:0002 p:0057 s:0005 e:001d40 EVAL testpcaprub.rb:9 [FINISH]
c:0001 p:0000 s:0002 e:00137c TOP [FINISH]

testpcaprub.rb:9:in <main>' testpcaprub.rb:9:in <>'
testpcaprub.rb:10:in block in <main>' testpcaprub.rb:10:in dump'

-- C level backtrace information -----
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(+0x18f603) [0xb7619603] vm_dump.c:644
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(+0x54f5b) [0xb74def5b] vfscanf.c:1965
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(rb_bug+0x44) [0xb74dfef4] ../sysdeps/posix/tempname.c:227
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(+0x118c54) [0xb75a2c54] des_impl.c:430
[0xb76ec40c]
/lib/i386-linux-gnu/libc.so.6(fwrite+0x35) [0xb7323775] iofwrite.c:41
/usr/lib/i386-linux-gnu/libpcap.so.0.8(pcap_dump+0x5d) [0xb6f68d5d] regexec.c:3465
/home/dario/.rvm/gems/ruby-2.0.0-preview1/gems/pcaprub-0.11.3/lib/pcaprub.so(+0x2626) [0xb7480626] pcaprub.c:500
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(+0x176969) [0xb7600969] vm_insnhelper.c:1329
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(+0x179f1a) [0xb7603f1a] vm_insnhelper.c:1442
```

```

/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(+0x186f39) [0xb7610f39] vm_insnhelper.c:1529
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(+0x17e747) [0xb7608747] insns.def:983
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(+0x183a18) [0xb760da18] vm.c:1153
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(rb_yield+0x1f7) [0xb7613fd7] vm.c:624
/home/dario/.rvm/gems/ruby-2.0.0-preview1/gems/pcaprub-0.11.3/lib/pcaprub.so(+0x1885) [0xb747f885] pcaprub.c:673
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(+0x1768e1) [0xb76008e1] vm_insnhelper.c:1311
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(+0x179f1a) [0xb7603f1a] vm_insnhelper.c:1442
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(+0x186f39) [0xb7610f39] vm_insnhelper.c:1529
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(+0x17e157) [0xb7608157] insns.def:968
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(+0x183a18) [0xb760da18] vm.c:1153
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(rb_iseq_eval_main+0xa2) [0xb7614a12] vm.c:1396
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(+0x59924) [0xb74e3924] vfprintf.c:1465
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(ruby_exec_node+0x24) [0xb74e4744] vfprintf.c:1629
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0(ruby_run_node+0x36) [0xb74e6766] vfprintf.c:2280
ruby() [0x8048658]
/lib/i386-linux-gnu/libc.so.6(__libc_start_main+0xf3) [0xb72d64d3] libc-start.c:226
ruby() [0x8048681]

```

-- Other runtime information -----

- Loaded script: testpcaprub.rb

- Loaded features:

0 enumerator.so

```

1 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/2.0.0/i686-linux/enc/encdb.so
2 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/2.0.0/i686-linux/enc/trans/transdb.so
3 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/site_ruby/2.0.0/rubygems/defaults.rb
4 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/2.0.0/i686-linux/rbconfig.rb
5 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/site_ruby/2.0.0/rubygems/deprecate.rb
6 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/site_ruby/2.0.0/rubygems/exceptions.rb
7 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/site_ruby/2.0.0/rubygems/custom_require.rb
8 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/site_ruby/2.0.0/rubygems.rb
9 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/site_ruby/2.0.0/rubygems/version.rb
10 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/site_ruby/2.0.0/rubygems/requirement.rb
11 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/site_ruby/2.0.0/rubygems/platform.rb
12 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/site_ruby/2.0.0/rubygems/specification.rb
13 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/site_ruby/2.0.0/rubygems/path_support.rb
14 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/site_ruby/2.0.0/rubygems/dependency.rb
15 /home/dario/.rvm/gems/ruby-2.0.0-preview1/gems/pcaprub-0.11.3/lib/pcaprub/common.rb
16 /home/dario/.rvm/gems/ruby-2.0.0-preview1/gems/pcaprub-0.11.3/lib/pcaprub/version.rb
17 /home/dario/.rvm/gems/ruby-2.0.0-preview1/gems/pcaprub-0.11.3/lib/pcaprub.so
18 /home/dario/.rvm/gems/ruby-2.0.0-preview1/gems/pcaprub-0.11.3/lib/pcaprub/ext.rb
19 /home/dario/.rvm/gems/ruby-2.0.0-preview1/gems/pcaprub-0.11.3/lib/pcaprub.rb

```

- Process memory map:

```

08048000-08049000 r-xp 00000000 08:01 13504431 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/bin/ruby
08049000-0804a000 r--p 00000000 08:01 13504431 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/bin/ruby
0804a000-0804b000 rw-p 00001000 08:01 13504431 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/bin/ruby
08fff000-09290000 rw-p 00000000 00:00 0 [heap]
b6b51000-b6b52000 rw-p 00000000 00:00 0
b6b52000-b6b6e000 r-xp 00000000 08:01 525236 /lib/i386-linux-gnu/libgcc_s.so.1
b6b6e000-b6b6f000 r--p 0001b000 08:01 525236 /lib/i386-linux-gnu/libgcc_s.so.1
b6b6f000-b6b70000 rw-p 0001c000 08:01 525236 /lib/i386-linux-gnu/libgcc_s.so.1
b6b70000-b6f50000 rw-s 00000000 00:07 6428389 socket:[6428389]
b6f50000-b6f84000 r-xp 00000000 08:01 7607152 /usr/lib/i386-linux-gnu/libpcap.so.1.1.1
b6f84000-b6f85000 ---p 00034000 08:01 7607152 /usr/lib/i386-linux-gnu/libpcap.so.1.1.1
b6f85000-b6f86000 r--p 00034000 08:01 7607152 /usr/lib/i386-linux-gnu/libpcap.so.1.1.1
b6f86000-b6f87000 rw-p 00035000 08:01 7607152 /usr/lib/i386-linux-gnu/libpcap.so.1.1.1
b6fab000-b6fad000 r-xp 00000000 08:01 13511690
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/2.0.0/i686-linux/enc/encdb.so
b6fad000-b6fae000 r--p 00001000 08:01 13511690
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/2.0.0/i686-linux/enc/encdb.so
b6fae000-b6faf000 rw-p 00002000 08:01 13511690
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/2.0.0/i686-linux/enc/encdb.so

```

```

b6faf000-b6fb0000 ---p 00000000 00:00 0
b6fb0000-b7034000 rw-p 00000000 00:00 0
b7034000-b7234000 r--p 00000000 08:01 7609336 /usr/lib/locale/locale-archive
b7234000-b7236000 rw-p 00000000 00:00 0
b7236000-b7260000 r-xp 00000000 08:01 533185 /lib/i386-linux-gnu/libm-2.15.so
b7260000-b7261000 r--p 00029000 08:01 533185 /lib/i386-linux-gnu/libm-2.15.so
b7261000-b7262000 rw-p 0002a000 08:01 533185 /lib/i386-linux-gnu/libm-2.15.so
b7262000-b726a000 r-xp 00000000 08:01 525257 /lib/i386-linux-gnu/libcrypt-2.15.so
b726a000-b726b000 r--p 00007000 08:01 525257 /lib/i386-linux-gnu/libcrypt-2.15.so
b726b000-b726c000 rw-p 00008000 08:01 525257 /lib/i386-linux-gnu/libcrypt-2.15.so
b726c000-b7293000 rw-p 00000000 00:00 0
b7293000-b7296000 r-xp 00000000 08:01 533189 /lib/i386-linux-gnu/libdl-2.15.so
b7296000-b7297000 r--p 00002000 08:01 533189 /lib/i386-linux-gnu/libdl-2.15.so
b7297000-b7298000 rw-p 00003000 08:01 533189 /lib/i386-linux-gnu/libdl-2.15.so
b7298000-b729f000 r-xp 00000000 08:01 533181 /lib/i386-linux-gnu/librt-2.15.so
b729f000-b72a0000 r--p 00006000 08:01 533181 /lib/i386-linux-gnu/librt-2.15.so
b72a0000-b72a1000 rw-p 00007000 08:01 533181 /lib/i386-linux-gnu/librt-2.15.so
b72a1000-b72b8000 r-xp 00000000 08:01 533183 /lib/i386-linux-gnu/libpthread-2.15.so
b72b8000-b72b9000 r--p 00016000 08:01 533183 /lib/i386-linux-gnu/libpthread-2.15.so
b72b9000-b72ba000 rw-p 00017000 08:01 533183 /lib/i386-linux-gnu/libpthread-2.15.so
b72ba000-b72bd000 rw-p 00000000 00:00 0
b72bd000-b7460000 r-xp 00000000 08:01 524409 /lib/i386-linux-gnu/libc-2.15.so
b7460000-b7462000 r--p 001a3000 08:01 524409 /lib/i386-linux-gnu/libc-2.15.so
b7462000-b7463000 rw-p 001a5000 08:01 524409 /lib/i386-linux-gnu/libc-2.15.so
b7463000-b7466000 rw-p 00000000 00:00 0
b747e000-b7483000 r-xp 00000000 08:01 13514394
/home/dario/.rvm/gems/ruby-2.0.0-preview1/gems/pcaprub-0.11.3/lib/pcaprub.so
b7483000-b7484000 r--p 00004000 08:01 13514394
/home/dario/.rvm/gems/ruby-2.0.0-preview1/gems/pcaprub-0.11.3/lib/pcaprub.so
b7484000-b7485000 rw-p 00005000 08:01 13514394
/home/dario/.rvm/gems/ruby-2.0.0-preview1/gems/pcaprub-0.11.3/lib/pcaprub.so
b7485000-b7487000 r-xp 00000000 08:01 13511697
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/2.0.0/i686-linux/enc/trans/transdb.so
b7487000-b7488000 r--p 00001000 08:01 13511697
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/2.0.0/i686-linux/enc/trans/transdb.so
b7488000-b7489000 rw-p 00002000 08:01 13511697
/home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/ruby/2.0.0/i686-linux/enc/trans/transdb.so
b7489000-b748a000 r--p 005e0000 08:01 7609336 /usr/lib/locale/locale-archive
b748a000-b76d1000 r-xp 00000000 08:01 13504432 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0.0
b76d1000-b76d4000 r--p 00246000 08:01 13504432 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0.0
b76d4000-b76d6000 rw-p 00249000 08:01 13504432 /home/dario/.rvm/rubies/ruby-2.0.0-preview1/lib/libruby.so.2.0.0
b76d6000-b76ec000 rw-p 00000000 00:00 0
b76ec000-b76ed000 r-xp 00000000 00:00 0 [vdso]
b76ed000-b770d000 r-xp 00000000 08:01 533186 /lib/i386-linux-gnu/ld-2.15.so
b770d000-b770e000 r--p 0001f000 08:01 533186 /lib/i386-linux-gnu/ld-2.15.so
b770e000-b770f000 rw-p 00020000 08:01 533186 /lib/i386-linux-gnu/ld-2.15.so
bfb76000-bfb97000 rw-p 00000000 00:00 0 [stack]

```

[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>

Dump is more or less the same in 1.9 while in 1.8 I just can see

testpcaprub.rb:10: [BUG] Segmentation fault

History

#1 - 05/14/2013 11:05 PM - crondaemon (Dario Lombardo)

Still present in

ruby 2.0.0p0 (2013-02-24 revision 39474) [x86_64-linux]

#2 - 05/19/2013 10:20 PM - nagachika (Tomoyuki Chikanaga)

- Status changed from Open to Third Party's Issue

Hello,

It seems that pcaprub contains an extension library and Segmentation fault was occurred inside it.
Please report this issue to pcaprub project.

Thanks,

#3 - 06/11/2013 10:09 PM - crondaemon (Dario Lombardo)

Reported. Please consider this issue closed, and sorry for the wrong report.