Ruby trunk - Bug #9523

marshal_dump and callcc causes SEGV

02/16/2014 11:05 PM - akr (Akira Tanaka)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.2.0dev (2014-02-17 trunk 45016) [x86_64-linux]	**Backport:**	1.9.3: DONTNEED, 2.0.0: DONTNEED, 2.1: DONTNEED

Description

```
Ruby dumps core as follows.
% ./ruby -rcontinuation -e '
class C
  def marshal_dump
    callcc {|c| $c = c }
    nil
  end
  def marshal_load(v)
  end
end
p Marshal.dump(C.new)
$c.call
'
"\x04\bU:\x06C0"
-e:10: [BUG] Segmentation fault at 0x00000000000001
ruby 2.2.0dev (2014-02-17 trunk 45016) [x86_64-linux]
-- Control frame information -----------------------------------------------
c:0003 p:---- s:0009 e:000008 CFUNC  :dump
c:0002 p:0031 s:0005 E:001e08 EVAL   -e:10 [FINISH]
c:0001 p:0000 s:0002 E:0008f8 TOP    [FINISH]
-- Ruby level backtrace information ----------------------------------------
-e:10:in `<main>'
-e:10:in `dump'
-- C level backtrace information -------------------------------------------
./ruby(+0x173e12) [0x7fa9014b7e12]
./ruby(+0x173ee7) [0x7fa9014b7ee7]
./ruby(+0x1cf3ff) [0x7fa9015133ff]
./ruby(rb_bug+0xdf) [0x7fa901513579]
./ruby(+0xececa) [0x7fa901430eca]
/lib/x86_64-linux-gnu/libpthread.so.0(+0xf210) [0x7fa900f13210] ../nptl/sysdeps/pthread/funlockfil
e.c:29
./ruby(st_lookup+0x18) [0x7fa90143ac13]
./ruby(+0x62e50) [0x7fa9013a6e50]
./ruby(+0x637a4) [0x7fa9013a77a4]
./ruby(+0x64988) [0x7fa9013a8988]
./ruby(+0x15a006) [0x7fa90149e006]
./ruby(+0x15abb5) [0x7fa90149ebb5]
./ruby(+0x15acc2) [0x7fa90149ecc2]
./ruby(+0x15b7a8) [0x7fa90149f7a8]
./ruby(+0x15c019) [0x7fa9014a0019]
./ruby(+0x15f908) [0x7fa9014a3908]
./ruby(+0x16f7e9) [0x7fa9014b37e9]
./ruby(rb_iseq_eval_main+0x34) [0x7fa9014b4756]
./ruby(+0x230c8) [0x7fa9013670c8]
./ruby(ruby_exec_node+0x24) [0x7fa9013671e1]
./ruby(ruby_run_node+0x3e) [0x7fa9013671b4]
./ruby(+0x21236) [0x7fa901365236]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf5) [0x7fa9001c8995] eval_error.c:65
./ruby(+0x210d9) [0x7fa9013650d9]
-- Other runtime information -----------------------------------------------
* Loaded script: -e
```

```
* Loaded features:
0 enumerator.so
1 /home/ruby/tst1/lib/ruby/2.2.0/x86_64-linux/enc/encdb.so
2 /home/ruby/tst1/lib/ruby/2.2.0/x86_64-linux/enc/trans/transdb.so
3 /home/ruby/tst1/lib/ruby/2.2.0/x86_64-linux/rbconfig.rb
4 /home/ruby/tst1/lib/ruby/2.2.0/rubygems/compatibility.rb
5 /home/ruby/tst1/lib/ruby/2.2.0/rubygems/defaults.rb
6 /home/ruby/tst1/lib/ruby/2.2.0/rubygems/deprecate.rb
7 /home/ruby/tst1/lib/ruby/2.2.0/rubygems/errors.rb
8 /home/ruby/tst1/lib/ruby/2.2.0/rubygems/version.rb
9 /home/ruby/tst1/lib/ruby/2.2.0/rubygems/requirement.rb
10 /home/ruby/tst1/lib/ruby/2.2.0/rubygems/platform.rb
11 /home/ruby/tst1/lib/ruby/2.2.0/rubygems/basic_specification.rb
12 /home/ruby/tst1/lib/ruby/2.2.0/rubygems/stub_specification.rb
13 /home/ruby/tst1/lib/ruby/2.2.0/rubygems/util/stringio.rb
14 /home/ruby/tst1/lib/ruby/2.2.0/rubygems/specification.rb
15 /home/ruby/tst1/lib/ruby/2.2.0/rubygems/exceptions.rb
16 /home/ruby/tst1/lib/ruby/2.2.0/rubygems/core_ext/kernel_gem.rb
17 thread.rb
18 /home/ruby/tst1/lib/ruby/2.2.0/x86_64-linux/thread.so
19 /home/ruby/tst1/lib/ruby/2.2.0/monitor.rb
20 /home/ruby/tst1/lib/ruby/2.2.0/rubygems/core_ext/kernel_require.rb
21 /home/ruby/tst1/lib/ruby/2.2.0/rubygems.rb
22 /home/ruby/tst1/lib/ruby/2.2.0/x86_64-linux/continuation.so
* Process memory map:
7fa8ff687000-7fa8ff69c000 r-xp 00000000 08:02 2883588                    /lib/x86_64-linux-gnu/lib
gcc_s.so.1
7fa8ff69c000-7fa8ff89c000 ---p 00015000 08:02 2883588                    /lib/x86_64-linux-gnu/lib
gcc_s.so.1
7fa8ff89c000-7fa8ff89d000 rw-p 00015000 08:02 2883588                    /lib/x86_64-linux-gnu/lib
gcc_s.so.1
7fa8ff89d000-7fa8ff89e000 r-xp 00000000 08:02 19663128                   /home/ruby/tst1/lib/ruby/
2.2.0/x86_64-linux/continuation.so
7fa8ff89e000-7fa8ffa9d000 ---p 00001000 08:02 19663128                   /home/ruby/tst1/lib/ruby/
2.2.0/x86_64-linux/continuation.so
7fa8ffa9d000-7fa8ffa9e000 rw-p 00000000 08:02 19663128                   /home/ruby/tst1/lib/ruby/
2.2.0/x86_64-linux/continuation.so
7fa8ffa9e000-7fa8ffaa1000 r-xp 00000000 08:02 19660804                   /home/ruby/tst1/lib/ruby/
2.2.0/x86_64-linux/thread.so
7fa8ffaa1000-7fa8ffca0000 ---p 00003000 08:02 19660804                   /home/ruby/tst1/lib/ruby/
2.2.0/x86_64-linux/thread.so
7fa8ffca0000-7fa8ffca1000 rw-p 00002000 08:02 19660804                   /home/ruby/tst1/lib/ruby/
2.2.0/x86_64-linux/thread.so
7fa8ffca1000-7fa8ffca3000 r-xp 00000000 08:02 19660862                   /home/ruby/tst1/lib/ruby/
2.2.0/x86_64-linux/enc/trans/transdb.so
7fa8ffca3000-7fa8ffea3000 ---p 00002000 08:02 19660862                   /home/ruby/tst1/lib/ruby/
2.2.0/x86_64-linux/enc/trans/transdb.so
7fa8ffea3000-7fa8ffea4000 rw-p 00002000 08:02 19660862                   /home/ruby/tst1/lib/ruby/
2.2.0/x86_64-linux/enc/trans/transdb.so
7fa8ffea4000-7fa8ffea6000 r-xp 00000000 08:02 19663116                   /home/ruby/tst1/lib/ruby/
2.2.0/x86_64-linux/enc/encdb.so
7fa8ffea6000-7fa9000a5000 ---p 00002000 08:02 19663116                   /home/ruby/tst1/lib/ruby/
2.2.0/x86_64-linux/enc/encdb.so
7fa9000a5000-7fa9000a6000 rw-p 00001000 08:02 19663116                   /home/ruby/tst1/lib/ruby/
2.2.0/x86_64-linux/enc/encdb.so
7fa9000a6000-7fa9001a7000 rw-p 00000000 00:00 0
7fa9001a7000-7fa90034a000 r-xp 00000000 08:02 2883602                    /lib/x86_64-linux-gnu/lib
c-2.17.so
7fa90034a000-7fa900549000 ---p 001a3000 08:02 2883602                    /lib/x86_64-linux-gnu/lib
c-2.17.so
7fa900549000-7fa90054d000 r--p 001a2000 08:02 2883602                    /lib/x86_64-linux-gnu/lib
c-2.17.so
7fa90054d000-7fa90054f000 rw-p 001a6000 08:02 2883602                    /lib/x86_64-linux-gnu/lib
c-2.17.so
7fa90054f000-7fa900553000 rw-p 00000000 00:00 0
7fa900553000-7fa90064f000 r-xp 00000000 08:02 2883608                    /lib/x86_64-linux-gnu/lib
m-2.17.so
```

```
7fa90064f000-7fa90084f000 ---p 000fc000 08:02 2883608                    /lib/x86_64-linux-gnu/lib
m-2.17.so
7fa90084f000-7fa900850000 r--p 000fc000 08:02 2883608                    /lib/x86_64-linux-gnu/lib
m-2.17.so
7fa900850000-7fa900851000 rw-p 000fd000 08:02 2883608                    /lib/x86_64-linux-gnu/lib
m-2.17.so
7fa900851000-7fa900859000 r-xp 00000000 08:02 2883607                    /lib/x86_64-linux-gnu/lib
crypt-2.17.so
7fa900859000-7fa900a58000 ---p 00008000 08:02 2883607                    /lib/x86_64-linux-gnu/lib
crypt-2.17.so
7fa900a58000-7fa900a59000 r--p 00007000 08:02 2883607                    /lib/x86_64-linux-gnu/lib
crypt-2.17.so
7fa900a59000-7fa900a5a000 rw-p 00008000 08:02 2883607                    /lib/x86_64-linux-gnu/lib
crypt-2.17.so
7fa900a5a000-7fa900a88000 rw-p 00000000 00:00 0
7fa900a88000-7fa900a8b000 r-xp 00000000 08:02 2883601                    /lib/x86_64-linux-gnu/lib
dl-2.17.so
7fa900a8b000-7fa900c8a000 ---p 00003000 08:02 2883601                    /lib/x86_64-linux-gnu/lib
dl-2.17.so
7fa900c8a000-7fa900c8b000 r--p 00002000 08:02 2883601                    /lib/x86_64-linux-gnu/lib
dl-2.17.so
7fa900c8b000-7fa900c8c000 rw-p 00003000 08:02 2883601                    /lib/x86_64-linux-gnu/lib
dl-2.17.so
7fa900c8c000-7fa900cfb000 r-xp 00000000 08:02 24908368                   /usr/lib/x86_64-linux-gnu
/libgmp.so.10.1.3
7fa900cfb000-7fa900efa000 ---p 0006f000 08:02 24908368                   /usr/lib/x86_64-linux-gnu
/libgmp.so.10.1.3
7fa900efa000-7fa900efb000 r--p 0006e000 08:02 24908368                   /usr/lib/x86_64-linux-gnu
/libgmp.so.10.1.3
7fa900efb000-7fa900f04000 rw-p 0006f000 08:02 24908368                   /usr/lib/x86_64-linux-gnu
/libgmp.so.10.1.3
7fa900f04000-7fa900f1b000 r-xp 00000000 08:02 2883595                    /lib/x86_64-linux-gnu/lib
pthread-2.17.so
7fa900f1b000-7fa90111a000 ---p 00017000 08:02 2883595                    /lib/x86_64-linux-gnu/lib
pthread-2.17.so
7fa90111a000-7fa90111b000 r--p 00016000 08:02 2883595                    /lib/x86_64-linux-gnu/lib
pthread-2.17.so
7fa90111b000-7fa90111c000 rw-p 00017000 08:02 2883595                    /lib/x86_64-linux-gnu/lib
pthread-2.17.so
7fa90111c000-7fa901120000 rw-p 00000000 00:00 0
7fa901120000-7fa901141000 r-xp 00000000 08:02 2883593                    /lib/x86_64-linux-gnu/ld-
2.17.so
7fa901219000-7fa901321000 r--p 00000000 08:02 24931804                   /usr/lib/locale/locale-ar
chive
7fa901321000-7fa901326000 rw-p 00000000 00:00 0
7fa90133a000-7fa90133b000 rw-p 00000000 00:00 0
7fa90133b000-7fa90133c000 ---p 00000000 00:00 0
7fa90133c000-7fa901341000 rw-p 00000000 00:00 0                          [stack:9285]
7fa901341000-7fa901342000 r--p 00021000 08:02 2883593                    /lib/x86_64-linux-gnu/ld-
2.17.so
7fa901342000-7fa901344000 rw-p 00022000 08:02 2883593                    /lib/x86_64-linux-gnu/ld-
2.17.so
7fa901344000-7fa9015e1000 r-xp 00000000 08:02 12981165                   /home/ruby/tst1/ruby/ruby
7fa9017e0000-7fa9017e6000 rw-p 0029c000 08:02 12981165                   /home/ruby/tst1/ruby/ruby
7fa9017e6000-7fa90180d000 rw-p 00000000 00:00 0
7fa903158000-7fa9035d4000 rw-p 00000000 00:00 0                          [heap]
7fffb3797000-7fffb37b8000 rw-p 00000000 00:00 0
7fffb37fe000-7fffb3800000 r-xp 00000000 00:00 0                          [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0                  [vsyscall]
[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
```

Related issues:

Related to Ruby trunk - Bug #7805: ruby 2.0rc2 core on solaris	**Closed**	**02/09/2013**

Associated revisions

Revision dd998dd5 - 02/17/2014 08:41 AM - nobu (Nobuyoshi Nakada)

marshal.c: do not recycle wrapper objects

- marshal.c (marshal_dump, marshal_load): do not recycle wrapper objects, to prevent from segfault with continuation. [ruby-dev:47970] [Bug #9523]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@45025 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 45025 - 02/17/2014 08:41 AM - nobu (Nobuyoshi Nakada)

marshal.c: do not recycle wrapper objects

- marshal.c (marshal_dump, marshal_load): do not recycle wrapper objects, to prevent from segfault with continuation. [ruby-dev:47970] [Bug #9523]

Revision 45025 - 02/17/2014 08:41 AM - nobu (Nobuyoshi Nakada)

marshal.c: do not recycle wrapper objects

- marshal.c (marshal_dump, marshal_load): do not recycle wrapper objects, to prevent from segfault with continuation. [ruby-dev:47970] [Bug #9523]

Revision 45025 - 02/17/2014 08:41 AM - nobu (Nobuyoshi Nakada)

marshal.c: do not recycle wrapper objects

- marshal.c (marshal_dump, marshal_load): do not recycle wrapper objects, to prevent from segfault with continuation. [ruby-dev:47970] [Bug #9523]

Revision 45025 - 02/17/2014 08:41 AM - nobu (Nobuyoshi Nakada)

marshal.c: do not recycle wrapper objects

- marshal.c (marshal_dump, marshal_load): do not recycle wrapper objects, to prevent from segfault with continuation. [ruby-dev:47970] [Bug #9523]

Revision 45025 - 02/17/2014 08:41 AM - nobu (Nobuyoshi Nakada)

marshal.c: do not recycle wrapper objects

- marshal.c (marshal_dump, marshal_load): do not recycle wrapper objects, to prevent from segfault with continuation. [ruby-dev:47970] [Bug #9523]

Revision 45025 - 02/17/2014 08:41 AM - nobu (Nobuyoshi Nakada)

marshal.c: do not recycle wrapper objects

- marshal.c (marshal_dump, marshal_load): do not recycle wrapper objects, to prevent from segfault with continuation. [ruby-dev:47970] [Bug #9523]

History

#1 - 02/16/2014 11:07 PM - akr (Akira Tanaka)

- Description updated

#2 - 02/17/2014 08:42 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

- % Done changed from 0 to 100

Applied in changeset r45025.

---

marshal.c: do not recycle wrapper objects

- marshal.c (marshal_dump, marshal_load): do not recycle wrapper objects, to prevent from segfault with continuation. [ruby-dev:47970] [Bug #9523]

#3 - 02/17/2014 08:50 AM - usa (Usaku NAKAMURA)

- Backport changed from 1.9.3: UNKNOWN, 2.0.0: UNKNOWN, 2.1: UNKNOWN to 1.9.3: DONTNEED, 2.0.0: DONTNEED, 2.1: DONTNEED

#4 - 02/18/2014 07:19 AM - ngoto (Naohisa Goto)

- Related to Bug #7805: ruby 2.0rc2 core on solaris added