

Ruby - Bug #1172

[sparc] *** glibc detected *** ruby1.9: free(): invalid pointer: 0xf7ef6a54 ***

02/18/2009 09:25 PM - lucas (Lucas Nussbaum)

Status:	Rejected	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	1.9.1p0	Backport:
Description =begin Hi, The following script causes the interpreter to crash on SPARC. It is likely to be caused by a mix of continuation and GC. <--- GC.start require 'continuation' o = Object.new def o.to_ary() callcc { k @cont = k; [1,2,3]} end GC.start begin if [10, 20, 1, 2, 3, 30, 1, 2, 3, 40] != [10, 20, o, 30, o, 40].flatten puts "FAIL1" exit(1) end GC.start puts "OK" rescue => e p e else puts "AA" o.instance_eval {@cont}.call end GC.start ---> Script output: <--- OK AA #<RuntimeError: flatten reentered> *** glibc detected *** ruby1.9: free(): invalid pointer: 0xf7f2aa54 *** Aborted ---> It fails both with: ruby 1.9.0 (2008-06-20 revision 17482) [sparc-linux] and ruby 1.9.1p0 (2009-01-30 revision 21907) [sparc-linux] =end		

History

#1 - 03/04/2009 02:15 AM - vipaca (Chad Dollins)

=begin
Please provide a core file.
=end

#2 - 03/04/2009 07:26 AM - lucas (Lucas Nussbaum)

=begin
Here is the full debug output:

*** glibc detected *** ruby1.9: free(): invalid pointer: 0xf7eeea54 ***

===== Backtrace: =====

/lib/libc.so.6(cfree+0x8c)[0xf7b4a12c]
/usr/lib/libruby1.9.so.1.9(ruby_xfree+0x28)[0xf7e297cc]
/usr/lib/libruby1.9.so.1.9[0xf7e2b248]
/usr/lib/libruby1.9.so.1.9(rb_gc+0x1c)[0xf7e2b5fc]
/usr/lib/libruby1.9.so.1.9(rb_gc_start+0x4)[0xf7e2b614]
/usr/lib/libruby1.9.so.1.9[0xf7ed62d4]
/usr/lib/libruby1.9.so.1.9[0xf7ed9088]
/usr/lib/libruby1.9.so.1.9[0xf7edaaac4]
/usr/lib/libruby1.9.so.1.9[0xf7ee0794]
/usr/lib/libruby1.9.so.1.9(rb_iseq_eval+0x16c)[0xf7ee099c]
/usr/lib/libruby1.9.so.1.9(ruby_exec_node+0x90)[0xf7e1bcf4]
/usr/lib/libruby1.9.so.1.9(ruby_run_node+0x40)[0xf7e1d2c4]
ruby1.9(main+0x54)[0x108cc]
/lib/libc.so.6(__libc_start_main+0x110)[0xf7ae7c50]
ruby1.9(_start+0x2c)[0x1072c]

===== Memory map: =====

00010000-00012000 r-xp 00000000 09:01 1144890
00020000-00022000 rwxp 00000000 09:01 1144890
00022000-000f0000 rwxp 00022000 00:00 0
f7692000-f7714000 rw-p f7692000 00:00 0
f7714000-f7716000 r-xp 00000000 09:01 1227352
f7716000-f7724000 ---p 00002000 09:01 1227352
f7724000-f7726000 rwxp 00000000 09:01 1227352
f7728000-f772a000 r-xp 00000000 09:01 1227317
f772a000-f7738000 ---p 00002000 09:01 1227317
f7738000-f773a000 rwxp 00000000 09:01 1227317
f773c000-f7740000 r-xp 00000000 09:01 1227321
f7740000-f774e000 ---p 00004000 09:01 1227321
f774e000-f7750000 rwxp 00002000 09:01 1227321
f7752000-f7754000 ---p f7752000 00:00 0
f7754000-f77da000 rw-p f7754000 00:00 0
f77da000-f77dc000 r-p 00dda000 09:01 1210076
f77de000-f78c8000 r-p 0019e000 09:01 1210076
f78c8000-f7ac8000 r-p 00000000 09:01 1210076
f7ac8000-f7c26000 r-xp 00000000 09:01 1148445
f7c26000-f7c36000 ---p 0015e000 09:01 1148445
f7c36000-f7c38000 r-p 0015e000 09:01 1148445
f7c38000-f7c3c000 rwxp 00160000 09:01 1148445
f7c3c000-f7c3e000 rwxp f7c3c000 00:00 0
f7c40000-f7d0e000 r-xp 00000000 09:01 1150019
f7d0e000-f7d1c000 ---p 000ce000 09:01 1150019
f7d1c000-f7d1e000 r-p 000cc000 09:01 1150019
f7d1e000-f7d22000 rwxp 000ce000 09:01 1150019
f7d24000-f7d2e000 r-xp 00000000 09:01 1148498
f7d2e000-f7d3c000 ---p 0000a000 09:01 1148498
f7d3c000-f7d3e000 r-p 00008000 09:01 1148498
f7d3e000-f7d40000 rwxp 0000a000 09:01 1148498
f7d40000-f7d66000 rwxp f7d40000 00:00 0
f7d68000-f7d6c000 r-xp 00000000 09:01 1148443
f7d6c000-f7d7a000 ---p 00004000 09:01 1148443
f7d7a000-f7d7c000 r-p 00002000 09:01 1148443
f7d7c000-f7d7e000 rwxp 00004000 09:01 1148443
f7d80000-f7d88000 r-xp 00000000 09:01 1148503
f7d88000-f7d96000 ---p 00008000 09:01 1148503
f7d96000-f7d98000 r-p 00006000 09:01 1148503
f7d98000-f7d9a000 rwxp 00008000 09:01 1148503
f7d9c000-f7db2000 r-xp 00000000 09:01 1148414
f7db2000-f7dc0000 ---p 00016000 09:01 1148414
f7dc0000-f7dc2000 r-p 00014000 09:01 1148414
f7dc2000-f7dc4000 rwxp 00016000 09:01 1148414
f7dc4000-f7dc6000 rwxp f7dc4000 00:00 0
f7dc8000-f7f2c000 r-xp 00000000 09:01 1144668
f7f2c000-f7f3a000 ---p 00164000 09:01 1144668
f7f3a000-f7f48000 rwxp 00162000 09:01 1144668
f7f48000-f7f58000 rwxp f7f48000 00:00 0
f7f68000-f7f8a000 r-xp 00000000 09:01 1150022
f7f96000-f7f98000 rw-p f7f96000 00:00 0
f7f98000-f7f9a000 r-p 00020000 09:01 1150022
f7f9a000-f7f9c000 rwxp 00022000 09:01 1150022
f7f9c000-f7f9e000 rw-p f7f9c000 00:00 0
ffdfa000-ffe24000 rw-p 7fefffd6000 00:00 0
Aborted (core dumped)

/usr/bin/ruby1.9
/usr/bin/ruby1.9
[heap]

/usr/lib/ruby/1.9.0/sparc-linux/continuation.so
/usr/lib/ruby/1.9.0/sparc-linux/continuation.so
/usr/lib/ruby/1.9.0/sparc-linux/continuation.so
/usr/lib/ruby/1.9.0/sparc-linux/enc/trans/transdb.so
/usr/lib/ruby/1.9.0/sparc-linux/enc/trans/transdb.so
/usr/lib/ruby/1.9.0/sparc-linux/enc/trans/transdb.so
/usr/lib/ruby/1.9.0/sparc-linux/enc/encdb.so
/usr/lib/ruby/1.9.0/sparc-linux/enc/encdb.so
/usr/lib/ruby/1.9.0/sparc-linux/enc/encdb.so

/usr/lib/locale/locale-archive
/usr/lib/locale/locale-archive
/usr/lib/locale/locale-archive
/lib/libc-2.9.so
/lib/libc-2.9.so
/lib/libc-2.9.so
/lib/libc-2.9.so

/lib/libm-2.9.so
/lib/libm-2.9.so
/lib/libm-2.9.so
/lib/libm-2.9.so
/lib/libcrypt-2.9.so
/lib/libcrypt-2.9.so
/lib/libcrypt-2.9.so
/lib/libcrypt-2.9.so

/lib/libdl-2.9.so
/lib/libdl-2.9.so
/lib/libdl-2.9.so
/lib/libdl-2.9.so
/lib/librt-2.9.so
/lib/librt-2.9.so
/lib/librt-2.9.so
/lib/librt-2.9.so
/lib/libpthread-2.9.so
/lib/libpthread-2.9.so
/lib/libpthread-2.9.so
/lib/libpthread-2.9.so

/usr/lib/libruby1.9.so.1.9.0
/usr/lib/libruby1.9.so.1.9.0
/usr/lib/libruby1.9.so.1.9.0

/lib/ld-2.9.so

/lib/ld-2.9.so
/lib/ld-2.9.so

[stack]

Do you have access to a SPARC ?

=end

#3 - 03/04/2009 01:44 PM - vipaca (Chad Dollins)

=begin
I do have access to a sparc and I will try your script for repro. However I was wondering if you could provide the core file associated with this segfault. It may not appear in your current directory because of process throttling. You can use 'ulimit -c ' if your shell is bash or limit -c I believe if you use csh. After the segfault you should see ./core file. please attach to issue.

Also I'm not quite sure how to get continuation compiled in to 1.9.1. Please leave details.

Thanks

Chad

=end

#4 - 03/05/2009 08:38 PM - lucas (Lucas Nussbaum)

=begin
I'm not comfortable with providing a core dump publicly, as it will leak information about the system I was using. I could send it to you via private mail, though. What's your email?

Regarding continuation in 1.9.1, it's there by default AFAIK. I didn't do anything special to get it compiled. I ran into the failure during the test suite (that is executed at the end of the Debian packages build), and then reduced it to the test case I described in the bug report.

See <http://experimental.debian.net/fetch.php?&pkg=ruby1.9&ver=1.9.1.0-1&arch=sparc&stamp=1235333763&file=log&as=raw>

And in particular:

TestArray#test_rindex: 0.00 s: .

TestArray#test_rindex2: 0.00 s: .

TestArray#test_sample: *** glibc detected *** ./ruby1.9: double free or corruption (out): 0x7022ef28 ***

===== Backtrace: =====

/lib/libc.so.6(cfree+0x8c)[0x7044612c]

/build/buildd/ruby1.9-1.9.1.0/libruby1.9-1.9.1.so.1.9.1[0x7015911c]

/build/buildd/ruby1.9-1.9.1.0/libruby1.9-1.9.1.so.1.9.1(rb_newobj+0x6c)[0x70159c9c]

[...]

=end

#5 - 03/07/2009 10:06 AM - vipaca (Chad Dollins)

=begin

Send me a copy to bug1172 at cdollins dot otherinbox dot com

=end

#6 - 03/07/2009 06:53 PM - lucas (Lucas Nussbaum)

=begin

sent

=end

#7 - 03/08/2009 06:40 PM - lucas (Lucas Nussbaum)

=begin

You wrote:

So I guess I'll take a different approach because this didn't work.

Please use gdb to decode the stack trace and attach this to the bug.

The stack trace is already available in that bug report (see comment #2).

=end

#8 - 03/09/2009 03:16 PM - vipaca (Chad Dollins)

=begin

I was looking for a decoded stack trace. If you can follow the directions I sent this should render the decode.

Thanks

Chad

=end

#9 - 03/09/2009 03:55 PM - lucas (Lucas Nussbaum)

=begin

(gdb) file ruby1.9

Reading symbols from /home/lucas/r191-0218/ruby1.9-1.9.1.0/ruby1.9...done.

```
(gdb) core ~/core.32505
Reading symbols from /usr/lib/libruby1.9.so.1.9...done.
Loaded symbols for /usr/lib/libruby1.9.so.1.9
Reading symbols from /lib/libpthread.so.0...done.
Loaded symbols for /lib/libpthread.so.0
Reading symbols from /lib/librt.so.1...done.
Loaded symbols for /lib/librt.so.1
Reading symbols from /lib/libdl.so.2...done.
Loaded symbols for /lib/libdl.so.2
Reading symbols from /lib/libcrypt.so.1...done.
Loaded symbols for /lib/libcrypt.so.1
Reading symbols from /lib/libm.so.6...done.
Loaded symbols for /lib/libm.so.6
Reading symbols from /lib/libc.so.6...done.
Loaded symbols for /lib/libc.so.6
Reading symbols from /lib/ld-linux.so.2...done.
Loaded symbols for /lib/ld-linux.so.2
Reading symbols from /usr/lib/ruby/1.9.0/sparc-linux/enc/encdb.so...done.
Loaded symbols for /usr/lib/ruby/1.9.0/sparc-linux/enc/encdb.so
Reading symbols from /usr/lib/ruby/1.9.0/sparc-linux/enc/trans/transdb.so...done.
Loaded symbols for /usr/lib/ruby/1.9.0/sparc-linux/enc/trans/transdb.so
Reading symbols from /usr/lib/ruby/1.9.0/sparc-linux/continuation.so...done.
Loaded symbols for /usr/lib/ruby/1.9.0/sparc-linux/continuation.so
Core was generated by `ruby1.9 t.rb'.
Program terminated with signal 6, Aborted.
[New process 32505]
[New process 32506]
#0  0xf7aff9cc in raise () from /lib/libc.so.6
(gdb) bt
#0  0xf7aff9cc in raise () from /lib/libc.so.6
#1  0x0000000c in ?? ()
#2  0x0000000c in ?? ()
Backtrace stopped: previous frame identical to this frame (corrupt stack?)
```

I don't think that we are going anywhere with this proxy debugging. You really need to (try to) reproduce the issue on a SPARC yourself. if you need access to a sparc, I can try to help, as I already said.
=end

#10 - 07/16/2009 05:45 PM - yugui (Yuki Sonoda)

```
=begin
A maintainer for Ruby on sparc is wanted.
=end
```

#11 - 10/11/2009 01:30 AM - naruse (Yui NARUSE)

- Status changed from Open to Rejected

```
=begin
SPARC is not supported.
=end
```