Ruby master - Bug #13758

TestRubyOptions#test_segv_setproctitle segfaults on AARCH64

07/20/2017 02:56 PM - vo.x (Vit Ondruch)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby -v: ruby 2.5.0dev (2017-07-20 trunk 59376) [aarch64-linux]	**Backport:**	2.2: UNKNOWN, 2.3: UNKNOWN, 2.4: UNKNOWN

Description

Or may be does not segfault properly?

```
  1) Failure:
TestRubyOptions#test_segv_setproctitle [/builddir/build/BUILD/ruby-2.5.0-r59376/test/ruby/test_rub
yoptions.rb:633]:
1. [2/2] Assertion for "stderr"
   | Expected /
   |         \[NOTE\]\n
   |         You\smay\shave\sencountered\sa\sbug\sin\sthe\sRuby\sinterpreter\sor\sextension\slibra
ries.\n
   |         Bug\sreports\sare\swelcome.\n
   |         (?:.*\n)?
   |         For\sdetails:\shttp:\/\/.*\.ruby-lang\.org\/.*\n
   |         \n
   |         (?:
   |           \[IMPORTANT\]\n
   |           (?:.+\n)+
   |           \n
   |         )?
   |       /x
   | to match
   |   "\n"+
   |   "-- Ruby level backtrace information ----------------------------------------\n"+
   |   "-e:1:in `<main>'\n"+
   |   "-e:1:in `kill'\n\n"+
   |   "-- C level backtrace information -------------------------------------------\n"+
   |   "/builddir/build/BUILD/ruby-2.5.0-r59376/libruby.so.2.5.0(rb_print_backtrace+0x20) [0xffff9
40b5a70] vm_dump.c:671\n"+
   |   "/builddir/build/BUILD/ruby-2.5.0-r59376/libruby.so.2.5.0(rb_vm_bugreport+0x8c) [0xffff940b
5b0c] vm_dump.c:941\n"+
   |   "/builddir/build/BUILD/ruby-2.5.0-r59376/libruby.so.2.5.0(rb_bug_context+0xb8) [0xffff93f92
528] error.c:534\n"+
   |   "/builddir/build/BUILD/ruby-2.5.0-r59376/libruby.so.2.5.0(sigsegv+0x4c) [0xffff9404c2e4] si
gnal.c:930\n"+
   |   "linux-vdso.so.1 [0xffff942096c0]\n"+
   |   "[0xffff93c230c8]\n"+
   |   "/builddir/build/BUILD/ruby-2.5.0-r59376/libruby.so.2.5.0(rb_f_kill+0x2c4) [0xffff9404d1bc]
 signal.c:498\n"+
   |   "/builddir/build/BUILD/ruby-2.5.0-r59376/libruby.so.2.5.0(vm_call_cfunc+0xec) [0xffff940a1e
34] vm_insnhelper.c:1889\n"+
   |   "/builddir/build/BUILD/ruby-2.5.0-r59376/libruby.so.2.5.0(vm_call_method+0xc8) [0xffff940ac
e90] ./include/ruby/ruby.h:1966\n"+
   |   "/builddir/build/BUILD/ruby-2.5.0-r59376/libruby.so.2.5.0(vm_exec_core+0x1490) [0xffff940a5
ab8] insns.def:856\n"+
   |   "/builddir/build/BUILD/ruby-2.5.0-r59376/libruby.so.2.5.0(vm_exec+0x84) [0xffff940a97bc] vm
_insnhelper.h:231\n"+
   |   "/builddir/build/BUILD/ruby-2.5.0-r59376/libruby.so.2.5.0(ruby_exec_internal+0xb4) [0xffff9
3f959c4] eval.c:244\n"+
   |   "/builddir/build/BUILD/ruby-2.5.0-r59376/libruby.so.2.5.0(ruby_exec_node+0x20) [0xffff93f97
808] eval.c:308\n"+
   |   "/builddir/build/BUILD/ruby-2.5.0-r59376/libruby.so.2.5.0(ruby_run_node+0x24) [0xffff93f995
```

```
fc] eval.c:300\n"+
   |   "/builddir/build/BUILD/ruby-2.5.0-r59376/ruby(main+0x50) [0xaaaad9048ac0] ./main.c:42\n\n"+
   |   "-- Other runtime information -----------------------------------------------\n\n"+
   |   "* Loaded script: /tmp/test_ruby_test_bug759720170720-12628-14djsbm.rb\n\n"+
   |   "* Loaded features:\n\n"+
   |   "    0 enumerator.so\n"+
   |   "    1 thread.rb\n"+
   |   "    2 rational.so\n"+
   |   "    3 complex.so\n"+
   |   "    4 /builddir/build/BUILD/ruby-2.5.0-r59376/.ext/aarch64-linux/enc/encdb.so\n"+
   |   "    5 /builddir/build/BUILD/ruby-2.5.0-r59376/.ext/aarch64-linux/enc/trans/transdb.so\n\n"
+
   |   "* Process memory map:\n\n"+
   |   "aaaad9048000-aaaad9049000 r-xp 00000000 fc:03 400504                   /builddir/build/B
UILD/ruby-2.5.0-r59376/ruby\n"+
   |   "aaaad9067000-aaaad9068000 r--p 0000f000 fc:03 400504                   /builddir/build/B
UILD/ruby-2.5.0-r59376/ruby\n"+
   |   "aaaad9068000-aaaad9069000 rw-p 00010000 fc:03 400504                   /builddir/build/B
UILD/ruby-2.5.0-r59376/ruby\n"+
   |   "aaaafb98e000-aaaafbacb000 rw-p 00000000 00:00 0                        [heap]\n"+
   |   "ffff92ded000-ffff93a26000 r--s 00000000 fc:03 400439                   /builddir/build/B
UILD/ruby-2.5.0-r59376/libruby.so.2.5.0\n"+
   |   "ffff93a26000-ffff93a39000 r--s 00000000 fc:03 400504                   /builddir/build/B
UILD/ruby-2.5.0-r59376/ruby\n"+
   |   "ffff93a39000-ffff93a4d000 r-xp 00000000 fc:03 1054631                  /usr/lib64/libgcc
_s-7-20170718.so.1\n"+
   |   "ffff93a4d000-ffff93a68000 ---p 00014000 fc:03 1054631                  /usr/lib64/libgcc
_s-7-20170718.so.1\n"+
   |   "ffff93a68000-ffff93a69000 r--p 0001f000 fc:03 1054631                  /usr/lib64/libgcc
_s-7-20170718.so.1\n"+
   |   "ffff93a69000-ffff93a6a000 rw-p 00020000 fc:03 1054631                  /usr/lib64/libgcc
_s-7-20170718.so.1\n"+
   |   "ffff93a6a000-ffff93a6c000 r-xp 00000000 fc:03 921755                   /builddir/build/B
UILD/ruby-2.5.0-r59376/.ext/aarch64-linux/enc/trans/transdb.so\n"+
   |   "ffff93a6c000-ffff93a89000 ---p 00002000 fc:03 921755                   /builddir/build/B
UILD/ruby-2.5.0-r59376/.ext/aarch64-linux/enc/trans/transdb.so\n"+
   |   "ffff93a89000-ffff93a8a000 r--p 0000f000 fc:03 921755                   /builddir/build/B
UILD/ruby-2.5.0-r59376/.ext/aarch64-linux/enc/trans/transdb.so\n"+
   |   "ffff93a8a000-ffff93a8b000 rw-p 00000000 00:00 0 \n"+
   |   "ffff93a8b000-ffff93a8d000 r-xp 00000000 fc:03 794844                   /builddir/build/B
UILD/ruby-2.5.0-r59376/.ext/aarch64-linux/enc/encdb.so\n"+
   |   "ffff93a8d000-ffff93aaa000 ---p 00002000 fc:03 794844                   /builddir/build/B
UILD/ruby-2.5.0-r59376/.ext/aarch64-linux/enc/encdb.so\n"+
   |   "ffff93aaa000-ffff93aab000 r--p 0000f000 fc:03 794844                   /builddir/build/B
UILD/ruby-2.5.0-r59376/.ext/aarch64-linux/enc/encdb.so\n"+
   |   "ffff93aab000-ffff93aac000 rw-p 00000000 00:00 0 \n"+
   |   "ffff93aac000-ffff93aad000 ---p 00000000 00:00 0 \n"+
   |   "ffff93aad000-ffff93bcd000 rw-p 00000000 00:00 0 \n"+
   |   "ffff93bcd000-ffff93bcf000 r-xp 00000000 fc:03 1055521                  /usr/lib64/libfre
ebl3.so\n"+
   |   "ffff93bcf000-ffff93bec000 ---p 00002000 fc:03 1055521                  /usr/lib64/libfre
ebl3.so\n"+
   |   "ffff93bec000-ffff93bed000 r--p 0000f000 fc:03 1055521                  /usr/lib64/libfre
ebl3.so\n"+
   |   "ffff93bed000-ffff93bee000 rw-p 00010000 fc:03 1055521                  /usr/lib64/libfre
ebl3.so\n"+
   |   "ffff93bee000-ffff93d77000 r-xp 00000000 fc:03 1055000                  /usr/lib64/libc-2
.25.90.so\n"+
   |   "ffff93d77000-ffff93d8a000 ---p 00189000 fc:03 1055000                  /usr/lib64/libc-2
.25.90.so\n"+
   |   "ffff93d8a000-ffff93d8e000 r--p 0018c000 fc:03 1055000                  /usr/lib64/libc-2
.25.90.so\n"+
   |   "ffff93d8e000-ffff93d90000 rw-p 00190000 fc:03 1055000                  /usr/lib64/libc-2
.25.90.so\n"+
   |   "ffff93d90000-ffff93d94000 rw-p 00000000 00:00 0 \n"+
   |   "ffff93d94000-ffff93e49000 r-xp 00000000 fc:03 1055006                  /usr/lib64/libm-2
.25.90.so\n"+
```

```
   |   "ffff93e49000-ffff93e63000 ---p 000b5000 fc:03 1055006                  /usr/lib64/libm-2
.25.90.so\n"+
   |   "ffff93e63000-ffff93e64000 r--p 000bf000 fc:03 1055006                  /usr/lib64/libm-2
.25.90.so\n"+
   |   "ffff93e64000-ffff93e65000 rw-p 000c0000 fc:03 1055006                  /usr/lib64/libm-2
.25.90.so\n"+
   |   "ffff93e65000-ffff93e6c000 r-xp 00000000 fc:03 1055524                  /usr/lib64/libcry
pt-nss-2.25.90.so\n"+
   |   "ffff93e6c000-ffff93e84000 ---p 00007000 fc:03 1055524                  /usr/lib64/libcry
pt-nss-2.25.90.so\n"+
   |   "ffff93e84000-ffff93e85000 r--p 0000f000 fc:03 1055524                  /usr/lib64/libcry
pt-nss-2.25.90.so\n"+
   |   "ffff93e85000-ffff93e86000 rw-p 00010000 fc:03 1055524                  /usr/lib64/libcry
pt-nss-2.25.90.so\n"+
   |   "ffff93e86000-ffff93eb4000 rw-p 00000000 00:00 0 \n"+
   |   "ffff93eb4000-ffff93eb7000 r-xp 00000000 fc:03 1055004                  /usr/lib64/libdl-
2.25.90.so\n"+
   |   "ffff93eb7000-ffff93ed3000 ---p 00003000 fc:03 1055004                  /usr/lib64/libdl-
2.25.90.so\n"+
   |   "ffff93ed3000-ffff93ed4000 r--p 0000f000 fc:03 1055004                  /usr/lib64/libdl-
2.25.90.so\n"+
   |   "ffff93ed4000-ffff93ed5000 rw-p 00010000 fc:03 1055004                  /usr/lib64/libdl-
2.25.90.so\n"+
   |   "ffff93ed5000-ffff93eef000 r-xp 00000000 fc:03 1055014                  /usr/lib64/libpth
read-2.25.90.so\n"+
   |   "ffff93eef000-ffff93f04000 ---p 0001a000 fc:03 1055014                  /usr/lib64/libpth
read-2.25.90.so\n"+
   |   "ffff93f04000-ffff93f05000 r--p 0001f000 fc:03 1055014                  /usr/lib64/libpth
read-2.25.90.so\n"+
   |   "ffff93f05000-ffff93f06000 rw-p 00020000 fc:03 1055014                  /usr/lib64/libpth
read-2.25.90.so\n"+
   |   "ffff93f06000-ffff93f0a000 rw-p 00000000 00:00 0 \n"+
   |   "ffff93f0a000-ffff94198000 r-xp 00000000 fc:03 400439                   /builddir/build/B
UILD/ruby-2.5.0-r59376/libruby.so.2.5.0\n"+
   |   "ffff94198000-ffff941b2000 ---p 0028e000 fc:03 400439                   /builddir/build/B
UILD/ruby-2.5.0-r59376/libruby.so.2.5.0\n"+
   |   "ffff941b2000-ffff941ba000 r--p 00298000 fc:03 400439                   /builddir/build/B
UILD/ruby-2.5.0-r59376/libruby.so.2.5.0\n"+
   |   "ffff941ba000-ffff941bb000 rw-p 002a0000 fc:03 400439                   /builddir/build/B
UILD/ruby-2.5.0-r59376/libruby.so.2.5.0\n"+
   |   "ffff941bb000-ffff941cb000 rw-p 00000000 00:00 0 \n"+
   |   "ffff941cb000-ffff941ed000 r-xp 00000000 fc:03 1054993                  /usr/lib64/ld-2.2
5.90.so\n"+
   |   "ffff941fd000-ffff94201000 rw-p 00000000 00:00 0 \n"+
   |   "ffff94206000-ffff94208000 rw-p 00000000 00:00 0 \n"+
   |   "ffff94208000-ffff94209000 r--p 00000000 00:00 0                        [vvar]\n"+
   |   "ffff94209000-ffff9420a000 r-xp 00000000 00:00 0                        [vdso]\n"+
   |   "ffff9420a000-ffff9420b000 r--p 0002f000 fc:03 1054993                  /usr/lib64/ld-2.2
5.90.so\n"+
   |   "ffff9420b000-ffff9420c000 rw-p 00030000 fc:03 1054993                  /usr/lib64/ld-2.2
5.90.so\n"+
   |   "ffff9420c000-ffff9420d000 rw-p 00000000 00:00 0 \n"+
   |   "fffffc21f000-fffffca1e000 rw-p 00000000 00:00 0                        [stack]\n"+
   |   "*** Error in `/tmp/test_ruby_test_bug759720170720-12628-14djsbm.rb': double free or corrup
tion (out): 0x0000aaaafba37fe0 ***\n"
   | after 6 patterns with 326 characters.
```

History

#1 - 09/01/2017 12:29 AM - naruse (Yui NARUSE)

- Status changed from Open to Feedback

I can't reproduce on ruby -v: ruby 2.5.0dev (2017-09-01 trunk 59707) [aarch64-linux].
see also http://rubyci.s3.amazonaws.com/scw-ad7f67/ruby-trunk/recent.html

#2 - 09/21/2017 10:32 AM - vo.x (Vit Ondruch)

naruse (Yui NARUSE) wrote:

> I can't reproduce on ruby -v: ruby 2.5.0dev (2017-09-01 trunk 59707) [aarch64-linux].
> see also http://rubyci.s3.amazonaws.com/scw-ad7f67/ruby-trunk/recent.html

You are using way older components then we do :/ I would blame glibc, binutils or something like that, since it seems the issue is in rb_print_backtrace or even in backtrace(void **trace, int size) function.

I think that the test case, although it should segfault, segfaults on different place then expected. IOW it segfaults in segfault handler ...

Trying to reproduce this on my computer (x86_64) with following steps:

```
$ ruby -e 'puts "f" * 100' > test_ruby_test_bug7597
$ ruby --disable-gems -e "$0=ARGV[0]; Process.kill :SEGV, $$" test_ruby_test_bug7597
```

it actually takes down the bash instance it is running within. Is this expected?

#3 - 09/21/2017 03:34 PM - Eregon (Benoit Daloze)

vo.x (Vit Ondruch) wrote:

> it actually takes down the bash instance it is running within. Is this expected?

Yes, Bash interprets the $$ inside the "":

```
echo "$$"
17490

echo '$$'
$$
```

#4 - 09/25/2017 08:15 AM - naruse (Yui NARUSE)

Eregon (Benoit Daloze) wrote:

> vo.x (Vit Ondruch) wrote:
>
> > it actually takes down the bash instance it is running within. Is this expected?
>
> Yes, Bash interprets the $$ inside the "":
>
> ```
> echo "$$"
> 17490
>
> echo '$$'
> $$
> ```

Therefore use Process.pid instead.

#5 - 10/11/2017 03:46 PM - vo.x (Vit Ondruch)

Eregon (Benoit Daloze) wrote:

> vo.x (Vit Ondruch) wrote:
>
> > it actually takes down the bash instance it is running within. Is this expected?
>
> Yes, Bash interprets the $$ inside the "":

Oh my, how could I ... Thx :)

Just FYI, I opened ticket with Fedora glibc maintainers, since it appears to be issue on some lower layer. I.e. it appears to fail in Kernel backtrace function 1 for some reasons.

Interestingly, I was not able to reproduce outside of the test suite :/

#6 - 10/11/2017 03:47 PM - vo.x (Vit Ondruch)

vo.x (Vit Ondruch) wrote:

> Just FYI, I opened ticket with Fedora glibc maintainers

Forgot to link the ticket: https://bugzilla.redhat.com/show_bug.cgi?id=1500863

#7 - 10/11/2017 03:50 PM - vo.x (Vit Ondruch)

BTW it seems that Ruby supports libunwind and we have libunwind available on Fedora. What would be the benefit of using it?

#8 - 10/12/2017 05:23 AM - vo.x (Vit Ondruch)

Can anybody help me we answer to glibc maintainers 1?

```
 Florian Weimer 2017-10-11 18:00:03 CEST

Does Ruby call backtrace from a signal handler?  It does on x86-64:

#0  __GI___backtrace (array=0x7f9c5cd12660, size=1024) at ../sysdeps/x86_64/backtrace.c:96
#1  0x00007f9c5ca27715 in rb_print_backtrace () from /lib64/libruby.so.2.4
#2  0x00007f9c5ca2794c in rb_vm_bugreport () from /lib64/libruby.so.2.4
#3  0x00007f9c5c900984 in rb_bug_context () from /lib64/libruby.so.2.4
#4  0x00007f9c5c9bce0e in sigsegv () from /lib64/libruby.so.2.4
#5  <signal handler called>
#6  0x00007f9c5ca16861 in vm_exec_core () from /lib64/libruby.so.2.4
#7  0x00007f9c5ca1b058 in vm_exec () from /lib64/libruby.so.2.4
#8  0x00007f9c5ca1bc11 in eval_string_with_cref () from /lib64/libruby.so.2.4
#9  0x00007f9c5ca1c068 in rb_f_eval () from /lib64/libruby.so.2.4

That's not valid in its own right because backtrace can call malloc, and the SIGSEGV handler might be called f
rom within malloc.

The backtrace issue we had on aarch64 has supposedly been fixed in rawhide:

https://sourceware.org/bugzilla/show_bug.cgi?id=21428
```

#9 - 10/12/2017 07:08 AM - normalperson (Eric Wong)

v.ondruch@tiscali.cz wrote:

> Can anybody help me we answer to glibc maintainers [1]?
>
> ```
>  Florian Weimer 2017-10-11 18:00:03 CEST
>
> Does Ruby call backtrace from a signal handler?  It does on x86-64:
> ```

Yes, it calls backtrace() unfortunately. It uses special signal
handlers for SIGILL, SIGSEGV, SIGBUS which sometimes screw up
debugging.

When tracking down some bugs in the past; I've flipped the value
of ruby_enable_coredump in signal.c to disable the nanny sighandlers
and get a real core dump.

(there's a more official way which involves re-running
./configure and using RUBY_DEBUG env; but that's too slow for my
hardware and I'd rather just recompile signal.o)

#10 - 12/14/2017 01:37 PM - vo.x (Vit Ondruch)

This is the glibc maintainer response 1:

> […]
>
> Okay, this makes it more of a Ruby bug, unfortunately.

It would be nice if this was fixed in Ruby.

#11 - 11/29/2018 02:14 PM - vo.x (Vit Ondruch)

Any chance to get this fixed? It is nice that Ruby has such fancy SIGSEGV handler, but it does not work on all platforms and it makes the matters just worse.

#12 - 01/09/2020 03:01 PM - vo.x (Vit Ondruch)

Was there some change/improvement in this area? I am trying Ruby 2.7.0 and I have not seen this issue during several past build attempts. Therefore I wonder if this was fixed or I am just lucky, because this used to fail annoyingly often.

#13 - 06/01/2020 09:39 PM - jeremyevans0 (Jeremy Evans)

- Status changed from Feedback to Closed