Ruby trunk - Bug #10389

SEGV after SEGV

10/15/2014 03:09 PM - akr (Akira Tanaka)

Status:	Closed		
Priority:	Normal		
Assignee:	nobu (Nobuyoshi Nakada)		
Target version:	2.2.0		
ruby -v:	ruby 2.2.0dev (2014-10-15 trunk 47951) [x86_64-linux]	**Backport:**	2.0.0: UNKNOWN, 2.1: UNKNOWN

Description

最近、SEGV したときに、さらに SEGV することがあります。

```
% ./miniruby -e 'Process.kill(:SEGV, $$)'
-e:1: [BUG] Segmentation fault at 0x0003e800003c63
ruby 2.2.0dev (2014-10-15 trunk 47951) [x86_64-linux]

-- Control frame information -----------------------------------------------
c:0003 p:---- s:0009 e:000008 CFUNC  :kill
c:0002 p:0015 s:0004 E:000080 EVAL   -e:1 [FINISH]
c:0001 p:0000 s:0002 E:0006f0 TOP    [FINISH]

-- Ruby level backtrace information ----------------------------------------
-e:1:in `<main>'
zsh: segmentation fault  ./miniruby -e 'Process.kill(:SEGV, $$)'
```

gdb で動かしてみると、RSTRING_PTR に 0 を渡しているようです。

```
% gdb miniruby
GNU gdb (Debian 7.7.1+dfsg-3) 7.7.1
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from miniruby...done.
(gdb) run -e 'Process.kill(:SEGV, $$)'
Starting program: /home/ruby/tst1/ruby/miniruby -e 'Process.kill(:SEGV, $$)'
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[New Thread 0x7ffff7ff5700 (LWP 15526)]

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff6e8d347 in kill () at ../sysdeps/unix/syscall-template.S:81
81  ../sysdeps/unix/syscall-template.S: そのようなファイルやディレクトリはありません .
(gdb) c
Continuing.
-e:1: [BUG] Segmentation fault at 0x0003e800003ca2
ruby 2.2.0dev (2014-10-15 trunk 47951) [x86_64-linux]

-- Control frame information -----------------------------------------------
c:0003 p:---- s:0009 e:000008 CFUNC  :kill
c:0002 p:0015 s:0004 E:0014e0 EVAL   -e:1 [FINISH]
c:0001 p:0000 s:0002 E:001ac0 TOP    [FINISH]
```

```
-- Ruby level backtrace information ----------------------------------------
-e:1:in `<main>'

Program received signal SIGSEGV, Segmentation fault.
0x000055555572f64c in oldbt_bugreport (arg=0x555555a8a78c, file=93824997590200, line=1, method=0)
at vm_backtrace.c:759
759     fprintf(stderr, "%s:%d:in `%s'\n", filename, line, RSTRING_PTR(method));
(gdb) p filename
$1 = 0x555555a704c8 "-e"
(gdb) p line
$2 = 1
(gdb) p method
$3 = 0
(gdb)
```

CI □□□□□□□□□□□□ r47914 □□□□□□□□□□□□
http://chkbuild002.hsbt.org/chkbuild/ruby-trunk/log/20141014T080011Z.diff.html.gz

Associated revisions

Revision 0ee11fc6 - 10/16/2014 01:45 PM - akr (Akira Tanaka)

- vm_backtrace.c (id2str): Fix a variable name. [ruby-dev:48642] [Bug #10389]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@47983 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 47983 - 10/16/2014 01:45 PM - akr (Akira Tanaka)

- vm_backtrace.c (id2str): Fix a variable name. [ruby-dev:48642] [Bug #10389]

Revision 47983 - 10/16/2014 01:45 PM - akr (Akira Tanaka)

- vm_backtrace.c (id2str): Fix a variable name. [ruby-dev:48642] [Bug #10389]

Revision 47983 - 10/16/2014 01:45 PM - akr (Akira Tanaka)

- vm_backtrace.c (id2str): Fix a variable name. [ruby-dev:48642] [Bug #10389]

Revision 47983 - 10/16/2014 01:45 PM - akr (Akira Tanaka)

- vm_backtrace.c (id2str): Fix a variable name. [ruby-dev:48642] [Bug #10389]

Revision 47983 - 10/16/2014 01:45 PM - akr (Akira Tanaka)

- vm_backtrace.c (id2str): Fix a variable name. [ruby-dev:48642] [Bug #10389]

Revision 47983 - 10/16/2014 01:45 PM - akr (Akira Tanaka)

- vm_backtrace.c (id2str): Fix a variable name. [ruby-dev:48642] [Bug #10389]

History

#1 - 10/16/2014 01:22 AM - nobu (Nobuyoshi Nakada)

- Category set to core

- Status changed from Open to Feedback

- Assignee set to nobu (Nobuyoshi Nakada)

- Target version set to 2.2.0

□□□ID□□□□□□□□□□□rb_id2str()□Qnil□□□□0□□□□□□□□□□□□
□□□r47951□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□ID□□□□□□□□□□□□□□□□□□

#2 - 10/16/2014 01:55 AM - akr (Akira Tanaka)

r47971 でも以下のように発生します。

```
% ./miniruby -e 'Process.kill(:SEGV, $$)'
-e:1: [BUG] Segmentation fault at 0x0003e80000389f
ruby 2.2.0dev (2014-10-16 trunk 47971) [x86_64-linux]

-- Control frame information -----------------------------------------------
c:0003 p:---- s:0009 e:000008 CFUNC  :kill
c:0002 p:0015 s:0004 E:0007f0 EVAL   -e:1 [FINISH]
c:0001 p:0000 s:0002 E:000e60 TOP    [FINISH]

-- Ruby level backtrace information ----------------------------------------
-e:1:in `<main>'
zsh: segmentation fault  ./miniruby -e 'Process.kill(:SEGV, $$)'
```

問題が発生した場合は SIGSEGV、発生しなかった場合は SIGABRT で終わるので以下のように数えると、
手元の Debian GNU/Linux (jessie) では、だいたい 20% くらいの確率で発生するようです。

```
% ./ruby -e '1000.times { system("./miniruby", "-e", "Process.kill(:SEGV, $$)", :err => "/dev/null"); puts Sig
nal.signame($?.termsig) }'|sort|uniq -c
    798 ABRT
    202 SEGV
% ./miniruby -v
ruby 2.2.0dev (2014-10-16 trunk 47971) [x86_64-linux]
```

#3 - 10/16/2014 01:40 PM - akr (Akira Tanaka)

Nobuyoshi Nakada wrote:

> 引数のIDが見つからないときにrb_id2str()がQnilではなく0を返すのは昔からです。
> そこはr47951で直したつもりなのですが、まだ起きるでしょうか。
>
> 存在するはずのIDが見つからないというのは別として。

もしかして、r47951 の

```
    VALUE str = rb_id2str(id);
    if (!id) return Qnil;
```

は

```
    VALUE str = rb_id2str(id);
    if (!str) return Qnil;
```

でしょうか。

#4 - 10/16/2014 01:46 PM - akr (Akira Tanaka)

- Status changed from Feedback to Closed

- % Done changed from 0 to 100

Applied in changeset r47983.

- vm_backtrace.c (id2str): Fix a variable name. [ruby-dev:48642] [Bug #10389]