Ruby trunk - Bug #6058

Stack overflow in SEGV Handler

02/22/2012 11:38 AM - authorNari (Narihiro Nakamura)

Status:	Closed		
Priority:	Normal		
Assignee:	kosaki (Motohiro KOSAKI)		
Target version:	2.0.0		
ruby -v:	ruby 2.0.0dev (2012-02-22 trunk 34726) [x86_64-linux]	**Backport:**	

Description

nariです。

以下のようにたまにSEGVのテストで落ちることがありまして、

http://c5664.rubyci.org/~chkbuild/ruby-trunk/log/20120221T130301Z.log.html.gz

原因を調査したところ、SIGSEGVハンドラの中でスタックオーバフローしている
ようでした。

```
# uname -orv
2.6.18-274.el5 #1 SMP Fri Jul 22 04:43:29 EDT 2011 GNU/Linux

# cat /etc/redhat-release
CentOS release 5.7 (Final)

# ./miniruby -v
ruby 2.0.0dev (2012-02-22 trunk 34726) [x86_64-linux]
```

64bit環境のCentOSだと100%再現しました。
./configureの指定はchkbuildと同じにしています。

```
# gdb ./miniruby
(gdb) r -e 'Process.kill :SIGSEGV, $$'
Starting program: /root/ruby/ruby-trunk-svn/miniruby -e 'Process.kill :SIGSEGV, $$'
warning: no loadable sections found in added symbol-file system-supplied DSO at 0x2aaaaaaab000
[Thread debugging using libthread_db enabled]
[New Thread 0x40003940 (LWP 5662)]

Program received signal SIGSEGV, Segmentation fault.
0x000000329b6306f7 in kill () from /lib64/libc.so.6
(gdb) c
Continuing.
-e:1: [BUG] Segmentation fault
ruby 2.0.0dev (2012-02-22 trunk 34726) [x86_64-linux]

-- Control frame information -----------------------------------------------

Program received signal SIGSEGV, Segmentation fault.
0x00002aaaae08d040 in ?? ()
(gdb) up
#1  0x00000000004e6304 in st_lookup (table=0x7f7a90, key=8368, value=0x7fa0e8) at st.c:399
399         hash_val = do_hash(key, table);
(gdb) p table
$1 = (st_table *) 0x7f7a90
(gdb) p *table
$2 = {type = 0x2aaaae18cf08, num_bins = 217355419913, entries_packed = 0, num_entries = 1664379390147606789, bins =
0x2820766564302e30, head = 0x2d32302d32313032,
tail = 0x6b6e757274203232}
(gdb) up
#2  0x0000000000490077 in rb_id2str (id=8368) at parse.y:10612
10612       if (st_lookup(global_symbols.id_str, id, &data)) {
```

```
(gdb) p global_symbols.id_str
$3 = (st_table *) 0x7f7a90
```

gdb□□□□□□global_symbols.id_str□□□□□□□□□□□□□□□□□
□□□□□□□□□

```
(gdb) (gdb) watch (((st_table *) 0x7f7a90)->type == 0x7d61f0)
Hardware watchpoint 2: (((st_table *) 0x7f7a90)->type == 0x7d61f0)
(gdb) r
...
Old value = 1
New value = 0
0x000000329b642841 in vfprintf () from /lib64/libc.so.6
(gdb) info frame
Stack level 0, Stack frame at 0x7f7aa0:
rip = 0x329b642841 in vfprintf; saved rip 0x329b648086
called by frame at 0x7f9bf0
Arglist at 0x7f7a90, args:
Locals at 0x7f7a90, Previous frame's sp is 0x7f7aa0
Saved registers:
rbp at 0x7f7a90, rip at 0x7f7a98
```

□□□□□□□□□□□□□□□□□□□□vfprintf()□□□□□□□□□□□
□□□□□□□□□□□□Locals□□□□□□global_symbols.id_str□□□□
□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□

Related issues:

Related to Ruby trunk - Bug #7141: ALT_STACK_SIZE is not enough	**Closed**	**10/11/2012**

Associated revisions

Revision d068ac8e - 02/25/2012 08:37 PM - naruse (Yui NARUSE)

- error.c (report_bug): use buf and snprintf to avoid consuming stack. [ruby-dev:45272] [Bug #6058]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@34817 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 34817 - 02/25/2012 08:37 PM - naruse (Yui NARUSE)

- error.c (report_bug): use buf and snprintf to avoid consuming stack. [ruby-dev:45272] [Bug #6058]

Revision 34817 - 02/25/2012 08:37 PM - naruse (Yui NARUSE)

- error.c (report_bug): use buf and snprintf to avoid consuming stack. [ruby-dev:45272] [Bug #6058]

Revision 34817 - 02/25/2012 08:37 PM - naruse (Yui NARUSE)

- error.c (report_bug): use buf and snprintf to avoid consuming stack. [ruby-dev:45272] [Bug #6058]

Revision 34817 - 02/25/2012 08:37 PM - naruse (Yui NARUSE)

- error.c (report_bug): use buf and snprintf to avoid consuming stack. [ruby-dev:45272] [Bug #6058]

Revision 34817 - 02/25/2012 08:37 PM - naruse (Yui NARUSE)

- error.c (report_bug): use buf and snprintf to avoid consuming stack. [ruby-dev:45272] [Bug #6058]

Revision 34817 - 02/25/2012 08:37 PM - naruse (Yui NARUSE)

- error.c (report_bug): use buf and snprintf to avoid consuming stack. [ruby-dev:45272] [Bug #6058]

History

#1 - 02/22/2012 12:37 PM - kosaki (Motohiro KOSAKI)

- Status changed from Open to Assigned

- Assignee set to kosaki (Motohiro KOSAKI)

□□□SEGV□□□□□□□□printf□□□□□□□□printf□□
ALT
STACK□□PROT_NONE□□
□□□□□□□□□□□□

#2 - 02/22/2012 01:04 PM - authorNari (Narihiro Nakamura)

Motohiro KOSAKI wrote:

> □□□SEGV□□□□□□□□printf□□□□□□□□printf□□□
> □□□□ALT
> STACK□□PROT_NONE□□
> □□□□□□□□□□□□□□□□□

□□□□□□□□□□□□ gdb□□□□□□□□□□□□□□□□□□□□

(gdb) r -e 'Process.kill :SIGSEGV, $$'
Starting program: /root/ruby/ruby-trunk-svn/miniruby -e 'Process.kill :SIGSEGV, $$'
warning: no loadable sections found in added symbol-file system-supplied DSO at 0x2aaaaaaab000
[Thread debugging using libthread_db enabled]
[New Thread 0x40003940 (LWP 5991)]

Program received signal SIGSEGV, Segmentation fault.
0x000000329b6306f7 in kill () from /lib64/libc.so.6
(gdb) c
Continuing.
-e:1: [BUG] Segmentation fault
ruby 2.0.0dev (2012-02-22 trunk 34726) [x86_64-linux]

-- Control frame information ---

Program received signal SIGSEGV, Segmentation fault.
0x00002aaaae08d040 in ?? ()
(gdb) bt
#0 0x00002aaaae08d040 in ?? ()
#1 0x00000000004e6304 in st_lookup (table=0x7f7a90, key=8368, value=0x7fa0e8) at st.c:399
#2 0x0000000000490077 in rb_id2str (id=8368) at parse.y:10612
#3 0x0000000000490159 in rb_id2name (id=8368) at parse.y:10643
#4 0x000000000053d893 in control_frame_dump (th=0x7f5520, cfp=0x2aaaae18ceb0) at vm_dump.c:121
#5 rb_vmdebug_stack_dump_raw (th=0x7f5520, cfp=0x2aaaae18ceb0) at vm_dump.c:182
#6 0x000000000053da6c in rb_vm_bugreport () at vm_dump.c:791
#7 0x00000000004446fe in report_bug (file=, line=, fmt=0x56a343 "Segmentation fault", args=0x7fa4d0) at error.c:266
#8 0x0000000000444878 in rb_bug (fmt=0x56a343 "Segmentation fault") at error.c:285
#9 0x00000000004df5d7 in sigsegv (sig=, info=, ctx=) at signal.c:603
#10
#11 0x000000329b6306f7 in kill () from /lib64/libc.so.6
#12 0x00000000004e049e in rb_f_kill (argc=2, argv=0x2aaaae08d048) at signal.c:397
#13 0x0000000000531720 in vm_call_cfunc (th=0x7f5520, cfp=0x2aaaae18cf08, num=, blockptr=0x1, flag=0, id=8368, me=0x8ed620, recv=8698280)
at vm_insnhelper.c:452
at vm_insnhelper.c:452
#14 vm_call_method (th=0x7f5520, cfp=0x2aaaae18cf08, num=, blockptr=0x1, flag=0, id=8368, me=0x8ed620, recv=8698280) at vm_insnhelper.c:578
#15 0x00000000005345ef in vm_exec_core (th=0x7f5520, initial=) at insns.def:1018
#16 0x0000000000539372 in vm_exec (th=0x7f5520) at vm.c:1223
#17 0x0000000000539601 in rb_iseq_eval_main (iseqval=8670360) at vm.c:1463
#18 0x0000000000447142 in ruby_exec_internal (n=0x844c98) at eval.c:204
#19 0x0000000000447169 in ruby_exec_node (n=0x844c98) at eval.c:251
#20 0x00000000004485cf in ruby_run_node (n=0x844c98) at eval.c:244
#21 0x0000000000415f63 in main (argc=3, argv=0x7fffffffe9e8) at main.c:38

#3 - 02/26/2012 05:37 AM - naruse (Yui NARUSE)

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r34817.
Narihiro, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- error.c (report_bug): use buf and snprintf to avoid consuming stack. [ruby-dev:45272] [Bug #6058]

#4 - 02/26/2012 05:44 AM - kosaki (Motohiro KOSAKI)

- Status changed from Closed to Assigned

workaroundとしてはこれで直りそうですが、元々のSEGVがあんまりなっとくいってないのでしばらく開き続けさせてください。ひまが出来たら追っかける

#5 - 02/26/2012 05:48 AM - kosaki (Motohiro KOSAKI)

ああ、思い出した。もともと buf[256] をここで使ってなかったのは

・ファイル名、行番号はスクリプト依存なので非常に長いファイル名を故意に生成可能なので二重SEGVを防ぐために上限を決める必要がある。ふつうファイル名は256程度で十分だろう
・fmt引数はRuby本体からわたされるので、長すぎるfmtがわたされたら呼び出し側のバグだろう

という意図でした。なので、256のままでいいのかちょっと自信がありません。たぶん大丈夫だと思いますが

#6 - 02/26/2012 02:58 PM - authorNari (Narihiro Nakamura)

r34817 の修正で私の手元でも直っていることを確認しました（ありがとうございます！）。
一応ご報告しておきます。

#7 - 12/15/2012 11:38 PM - kosaki (Motohiro KOSAKI)

- Status changed from Assigned to Closed

#7141 で理由が判明したのでcloseします