Ruby master - Bug #4312

exec cause Segmentation fault if passing very long string

01/24/2011 09:45 PM - kosaki (Motohiro KOSAKI)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:	1.9.3		
ruby -v:	ruby 1.9.3dev (2011-01-24 trunk 30642) [x86_64-linux]	**Backport:**	

Description

=begin
% ./ruby -ve 'exec "a"*100_000_000'

ruby 1.9.3dev (2011-01-24 trunk 30642) [x86_64-linux]
-e:1: [BUG] Segmentation fault
ruby 1.9.3dev (2011-01-24 trunk 30642) [x86_64-linux]

-- Control frame information ---
c:0004 p:---- s:0010 b:0010 l:000009 d:000009 CFUNC :exec
c:0003 p:0015 s:0006 b:0006 l:0025f8 d:000638 EVAL   -e:1
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:0025f8 d:0025f8 TOP

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

-- C level backtrace information ---
./ruby() [0x520595] vm_dump.c:797
./ruby() [0x564766] error.c:249
./ruby(rb_bug+0xb1) [0x564901] error.c:266
./ruby() [0x4af160] signal.c:624
/lib64/libpthread.so.0() [0x382140f440]
./ruby(rb_proc_exec+0x130) [0x4738f0] process.c:1150
./ruby(rb_f_exec+0x158) [0x475de8] process.c:2375
./ruby() [0x50f727] vm_insnhelper.c:403
./ruby() [0x5110a6] insns.def:1010
./ruby() [0x515e5b] vm.c:1150
./ruby(rb_iseq_eval_main+0x294) [0x516294] vm.c:1391
./ruby() [0x414f32] eval.c:225
./ruby(ruby_run_node+0x36) [0x416c66] eval.c:272
./ruby() [0x414129] main.c:38
/lib64/libc.so.6(__libc_start_main+0xfd) [0x3820c1ec5d]
./ruby() [0x414019]

-- Other runtime information ---

- Loaded script: -e
- Loaded features:

  0 enumerator.so
  1 /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/encdb.so
  2 /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/trans/transdb.so
  3 /usr/local/lib/ruby/1.9.1/rubygems/defaults.rb
  4 /usr/local/lib/ruby/1.9.1/thread.rb
  5 /usr/local/lib/ruby/1.9.1/x86_64-linux/etc.so
  6 /usr/local/lib/ruby/1.9.1/x86_64-linux/rbconfig.rb
  7 /usr/local/lib/ruby/1.9.1/rubygems/exceptions.rb
  8 /usr/local/lib/ruby/1.9.1/rubygems/version.rb
  9 /usr/local/lib/ruby/1.9.1/rubygems/requirement.rb

10 /usr/local/lib/ruby/1.9.1/rubygems/dependency.rb
11 /usr/local/lib/ruby/1.9.1/rubygems/gem_path_searcher.rb
12 /usr/local/lib/ruby/1.9.1/rubygems/user_interaction.rb
13 /usr/local/lib/ruby/1.9.1/rubygems/platform.rb
14 /usr/local/lib/ruby/1.9.1/rubygems/specification.rb
15 /usr/local/lib/ruby/1.9.1/rubygems/source_index.rb
16 /usr/local/lib/ruby/1.9.1/rubygems/builder.rb
17 /usr/local/lib/ruby/1.9.1/rubygems/config_file.rb
18 /usr/local/lib/ruby/1.9.1/rubygems/custom_require.rb
19 /usr/local/lib/ruby/1.9.1/rubygems.rb

- Process memory map:

```
00400000-00614000 r-xp 00000000 fd:03 2764210                    /home/kosaki/linux/ruby-svn/ruby/ruby
00814000-00816000 rw-p 00214000 fd:03 2764210                    /home/kosaki/linux/ruby-svn/ruby/ruby
00816000-0082e000 rw-p 00000000 00:00 0
00ea7000-0120f000 rw-p 00000000 00:00 0                          [heap]
3820800000-382081e000 r-xp 00000000 fd:00 4980746                /lib64/ld-2.12.1.so
3820a1e000-3820a1f000 r--p 0001e000 fd:00 4980746                /lib64/ld-2.12.1.so
3820a1f000-3820a20000 rw-p 0001f000 fd:00 4980746                /lib64/ld-2.12.1.so
3820a20000-3820a21000 rw-p 00000000 00:00 0
3820c00000-3820d75000 r-xp 00000000 fd:00 4980750                /lib64/libc-2.12.1.so
3820d75000-3820f75000 ---p 00175000 fd:00 4980750                /lib64/libc-2.12.1.so
3820f75000-3820f79000 r--p 00175000 fd:00 4980750                /lib64/libc-2.12.1.so
3820f79000-3820f7a000 rw-p 00179000 fd:00 4980750                /lib64/libc-2.12.1.so
3820f7a000-3820f7f000 rw-p 00000000 00:00 0
3821000000-3821002000 r-xp 00000000 fd:00 4981169                /lib64/libdl-2.12.1.so
3821002000-3821202000 ---p 00002000 fd:00 4981169                /lib64/libdl-2.12.1.so
3821202000-3821203000 r--p 00002000 fd:00 4981169                /lib64/libdl-2.12.1.so
3821203000-3821204000 rw-p 00003000 fd:00 4981169                /lib64/libdl-2.12.1.so
3821400000-3821417000 r-xp 00000000 fd:00 4980760                /lib64/libpthread-2.12.1.so
3821417000-3821616000 ---p 00017000 fd:00 4980760                /lib64/libpthread-2.12.1.so
3821616000-3821617000 r--p 00016000 fd:00 4980760                /lib64/libpthread-2.12.1.so
3821617000-3821618000 rw-p 00017000 fd:00 4980760                /lib64/libpthread-2.12.1.so
3821618000-382161c000 rw-p 00000000 00:00 0
3821800000-3821883000 r-xp 00000000 fd:00 4980786                /lib64/libm-2.12.1.so
3821883000-3821a82000 ---p 00083000 fd:00 4980786                /lib64/libm-2.12.1.so
3821a82000-3821a83000 r--p 00082000 fd:00 4980786                /lib64/libm-2.12.1.so
3821a83000-3821a84000 rw-p 00083000 fd:00 4980786                /lib64/libm-2.12.1.so
3821c00000-3821c07000 r-xp 00000000 fd:00 4980767                /lib64/librt-2.12.1.so
3821c07000-3821e06000 ---p 00007000 fd:00 4980767                /lib64/librt-2.12.1.so
3821e06000-3821e07000 r--p 00006000 fd:00 4980767                /lib64/librt-2.12.1.so
3821e07000-3821e08000 rw-p 00007000 fd:00 4980767                /lib64/librt-2.12.1.so
3825800000-3825816000 r-xp 00000000 fd:00 4980769                /lib64/libgcc_s-4.4.4-20100503.so.1
3825816000-3825a15000 ---p 00016000 fd:00 4980769                /lib64/libgcc_s-4.4.4-20100503.so.1
3825a15000-3825a16000 rw-p 00015000 fd:00 4980769                /lib64/libgcc_s-4.4.4-20100503.so.1
3831000000-3831058000 r-xp 00000000 fd:00 4981182                /lib64/libfreebl3.so
3831058000-3831257000 ---p 00058000 fd:00 4981182                /lib64/libfreebl3.so
3831257000-3831259000 rw-p 00057000 fd:00 4981182                /lib64/libfreebl3.so
3831259000-383125d000 rw-p 00000000 00:00 0
3831800000-3831807000 r-xp 00000000 fd:00 4981183                /lib64/libcrypt-2.12.1.so
3831807000-3831a07000 ---p 00007000 fd:00 4981183                /lib64/libcrypt-2.12.1.so
3831a07000-3831a08000 r--p 00007000 fd:00 4981183                /lib64/libcrypt-2.12.1.so
3831a08000-3831a09000 rw-p 00008000 fd:00 4981183                /lib64/libcrypt-2.12.1.so
3831a09000-3831a37000 rw-p 00000000 00:00 0
7f87ee887000-7f87f47e6000 rw-p 00000000 00:00 0
7f87f47e6000-7f87f47e9000 r-xp 00000000 fd:00 920209             /usr/local/lib/ruby/1.9.1/x86_64-linux/etc.so
7f87f47e9000-7f87f49e8000 ---p 00003000 fd:00 920209             /usr/local/lib/ruby/1.9.1/x86_64-linux/etc.so
7f87f49e8000-7f87f49e9000 rw-p 00002000 fd:00 920209             /usr/local/lib/ruby/1.9.1/x86_64-linux/etc.so
7f87f49e9000-7f87f49eb000 r-xp 00000000 fd:00 930967             /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/trans/transdb.so
7f87f49eb000-7f87f4bea000 ---p 00002000 fd:00 930967             /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/trans/transdb.so
7f87f4bea000-7f87f4beb000 rw-p 00001000 fd:00 930967             /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/trans/transdb.so
7f87f4beb000-7f87f4bed000 r-xp 00000000 fd:00 930968             /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/encdb.so
7f87f4bed000-7f87f4dec000 ---p 00002000 fd:00 930968             /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/encdb.so
7f87f4dec000-7f87f4ded000 rw-p 00001000 fd:00 930968             /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/encdb.so
7f87f4ded000-7f87f4dee000 rw-p 00000000 00:00 0
```

```
7f87f4dee000-7f87f4def000 ---p 00000000 00:00 0
7f87f4def000-7f87f4ef3000 rw-p 00000000 00:00 0
7f87f4ef3000-7f87fad84000 r--p 00000000 fd:00 321758                     /usr/lib/locale/locale-archive
7f87fad84000-7f87fad89000 rw-p 00000000 00:00 0
7f87fada6000-7f87fada8000 rw-p 00000000 00:00 0
7fff0f62c000-7fff0f641000 rw-p 00000000 00:00 0                          [stack]
7fff0f7ff000-7fff0f800000 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
=end
```

History

#1 - 01/24/2011 09:47 PM - kosaki (Motohiro KOSAKI)

=begin
Because rb_proc_exec() are using alloca and it can cause stack overflow. It shouldn't.
=end

#2 - 01/27/2011 08:47 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

- % Done changed from 0 to 100

=begin
This issue was solved with changeset r30662.
Motohiro, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- process.c (proc_exec_v, rb_proc_exec_n, rb_proc_exec) (proc_spawn_n, proc_spawn): get rid of too huge alloca(). [ruby-core:34827], [ruby-core:34833] =end