

Ruby - Bug #8946

Segmentation fault while NoMemoryError expected

09/24/2013 04:29 PM - tmqhliu (Xiaoding Liu)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 2.0.0p247 (2013-06-27) [x64-mingw32]	Backport: 2.2: UNKNOWN, 2.3: UNKNOWN, 2.4: UNKNOWN

Description

I was trying to watch gc behavior by generating NoMemoryError intentionally, a segmentation fault occurred without any exception raised.

the simple ruby code goes here:

```
arr= []

begin
  while true
    arr << 1
  end
rescue NoMemoryError
  puts 'no memory'
  puts GC.count
end
```

here is the ruby command line output:

```
C:\Ruby200-x64\bin\ruby.exe -e $stdout.sync=true;$stderr.sync=true;load($0=ARGV.shift) C:/Users/liuxd/RubymineProjects/rubymine/rubytest/ruby_learn.rb
C:/Users/liuxd/RubymineProjects/rubytest/ruby_learn.rb:6: [BUG] Segmentation fault
ruby 2.0.0p247 (2013-06-27) [x64-mingw32]

-- Control frame information -----
c:0004 p:0021 s:0011 e:000010 TOP      C:/Users/liuxd/RubymineProjects/rubytest/ruby_learn.rb:6 [FINISH]
c:0003 p:---- s:0008 e:000007 CFUNC  :load
c:0002 p:0035 s:0004 E:000658 EVAL    -e:1 [FINISH]
c:0001 p:0000 s:0002 E:001788 TOP      [FINISH]

-e:1:in `<main>'
-e:1:in `load'
C:/Users/liuxd/RubymineProjects/rubytest/ruby_learn.rb:6:in `<top (required)>'

-- C level backtrace information -----
C:\Windows\SYSTEM32\ntdll.dll(NtWaitForSingleObject+0xa) [0x00000000772812FA]
C:\Windows\system32\KERNELBASE.dll(WaitForSingleObjectEx+0x9c) [0x0000007FEFD3910DC]
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(rb_vm_bugreport+0x9d) [0x000000006F28327D]
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(rb_name_err_mesg_new+0x838) [0x000000006F141DF8]
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(rb_bug+0x45) [0x000000006F142BA5]
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(rb_check_safe_str+0x18c) [0x000000006F208E5C]
[0x0000000000401A85]
C:\Windows\SYSTEM32\ntdll.dll(_C_specific_handler+0x9c) [0x00000000772485C8]
C:\Windows\SYSTEM32\ntdll.dll(RtlDecodePointer+0xad) [0x0000000077259D2D]
C:\Windows\SYSTEM32\ntdll.dll(RtlUnwindEx+0xbbf) [0x00000000772491CF]
C:\Windows\SYSTEM32\ntdll.dll(KiUserExceptionDispatcher+0x2e) [0x0000000077281248]
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(rb_ary_push+0x4c) [0x000000006F10C16C]
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(rb_vm_local_jump_error+0x3223) [0x000000006F273D33]
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(rb_vm_local_jump_error+0x5ed9) [0x000000006F2769E9]
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(rb_iseq_eval+0x193) [0x000000006F2801D3]
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(rb_rubylevel_errinfo+0x5ea) [0x000000006F14B83A]
```

```
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(rb_rubylevel_errinfo+0x11be) [0x000000006F14C40E]
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(rb_error_arity+0x125) [0x000000006F26E485]
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(rb_add_method_cfunc+0x5f2) [0x000000006F27DF22]
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(rb_vm_localjump_error+0x21c8) [0x000000006F272CD8]
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(rb_vm_localjump_error+0x5ed9) [0x000000006F2769E9]
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(rb_iseq_eval_main+0x1e0) [0x000000006F280400]
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(rb_check_copyable+0x31f6) [0x000000006F147AD6]
C:\Ruby200-x64\bin\x64-msvcrt-ruby200.dll(ruby_run_node+0x51) [0x000000006F14A421]
[0x0000000000402D14]
[0x00000000004013D7]
[0x00000000004014F8]
C:\Windows\system32\kernel32.dll(BaseThreadInitThunk+0xd) [0x0000000076C6652D]
```

-- Other runtime information -----

* Loaded script: C:/Users/liuxd/RubymineProjects/rubyttest/ruby_learn.rb

* Loaded features:

```
0 enumerator.so
1 C:/Ruby200-x64/lib/ruby/2.0.0/x64-mingw32/enc/encdb.so
2 C:/Ruby200-x64/lib/ruby/2.0.0/x64-mingw32/enc/gbk.so
3 C:/Ruby200-x64/lib/ruby/2.0.0/x64-mingw32/enc/trans/transdb.so
4 C:/Ruby200-x64/lib/ruby/2.0.0/x64-mingw32/rbconfig.rb
5 C:/Ruby200-x64/lib/ruby/2.0.0/rubygems/compatibility.rb
6 C:/Ruby200-x64/lib/ruby/2.0.0/rubygems/defaults.rb
7 C:/Ruby200-x64/lib/ruby/2.0.0/rubygems/deprecate.rb
8 C:/Ruby200-x64/lib/ruby/2.0.0/rubygems/errors.rb
9 C:/Ruby200-x64/lib/ruby/2.0.0/rubygems/version.rb
10 C:/Ruby200-x64/lib/ruby/2.0.0/rubygems/requirement.rb
11 C:/Ruby200-x64/lib/ruby/2.0.0/rubygems/platform.rb
12 C:/Ruby200-x64/lib/ruby/2.0.0/rubygems/specification.rb
13 C:/Ruby200-x64/lib/ruby/2.0.0/rubygems/exceptions.rb
14 C:/Ruby200-x64/lib/ruby/2.0.0/rubygems/defaults/operating_system.rb
15 C:/Ruby200-x64/lib/ruby/2.0.0/x64-mingw32/enc/utf_16le.so
16 C:/Ruby200-x64/lib/ruby/2.0.0/x64-mingw32/enc/trans/utf_16_32.so
17 C:/Ruby200-x64/lib/ruby/2.0.0/rubygems/core_ext/kernel_gem.rb
18 C:/Ruby200-x64/lib/ruby/2.0.0/rubygems/core_ext/kernel_require.rb
19 C:/Ruby200-x64/lib/ruby/2.0.0/rubygems.rb
```

[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>

This application has requested the Runtime to terminate it in an unusual way.

Please contact the application's support team for more information.

Process finished with exit code 3

History

#1 - 05/06/2016 11:51 PM - hsbt (Hiroshi SHIBATA)

- Description updated

- Backport changed from 1.9.3: UNKNOWN, 2.0.0: UNKNOWN to 2.2: UNKNOWN, 2.3: UNKNOWN, 2.4: UNKNOWN

#2 - 08/15/2019 10:47 PM - jeremyevans0 (Jeremy Evans)

- Status changed from Open to Closed

From my testing, this was fixed between Ruby 2.2 and 2.3. Starting with Ruby 2.3, instead of segfaulting, I get:

```
t.rb:5:in `<main>': index 268435456 too big (IndexError)
```