Ruby trunk - Bug #5375

[mingw32] segfault on WinXP SP3 with 1.9.3dev@33347

09/28/2011 05:48 AM - jonforums (Jon Forums)

Status:	Closed		
Priority:	Normal		
Assignee:	luislavena (Luis Lavena)		
Target version:	1.9.3		
ruby -v:	ruby 1.9.3dev (2011-09-27 revision 33347) [i386-mingw32]	**Backport:**	

Description

With 1.9.3dev@33347 I get a segfault when running gem --version on WinXP SP3 32bit (Home and Professional) when Ruby is built with TDM-GCC 4.6.1 and the RubyInstaller recipes.

The build passed make test-all TESTS='openssl fiddle psych' && make test

I am unable to replicate the failure in the following environments:

- Win7 Professional or Ultimate 32bit
- ruby 1.9.3dev@33347 built with TDM-GCC 4.5.2
- ruby 1.9.4dev@33350 built with TDM-GCC 4.6.1
- ruby 1.9.4dev@33350 built with gcc 4.6.1 on Arch Linux 3.0

```
C:>ruby --version
ruby 1.9.3dev (2011-09-27 revision 33347) [i386-mingw32]

C:>gem --version
c:/ruby19/lib/ruby/1.9.1/psych/scalar_scanner.rb:71: [BUG] Segmentation fault
ruby 1.9.3dev (2011-09-27 revision 33347) [i386-mingw32]

-- Control frame information -----------------------------------------------
c:0027 p:---- s:0138 b:0138 l:000137 d:000137 CFUNC  :Integer
c:0026 p:0185 s:0134 b:0134 l:000133 d:000133 METHOD c:/ruby19/lib/ruby/1.9.1/psych/scalar_scanner.rb:71
c:0025 p:0220 s:0129 b:0129 l:000128 d:000128 METHOD c:/ruby19/lib/ruby/1.9.1/psych/visitors/to_ruby.rb:46
c:0024 p:0030 s:0118 b:0118 l:000117 d:000117 METHOD c:/ruby19/lib/ruby/1.9.1/psych/visitors/visitor.rb:15
c:0023 p:0013 s:0114 b:0114 l:000113 d:000113 METHOD c:/ruby19/lib/ruby/1.9.1/psych/visitors/visitor.rb:5
c:0022 p:0012 s:0110 b:0110 l:000109 d:000109 METHOD c:/ruby19/lib/ruby/1.9.1/psych/visitors/to_ruby.rb:16
c:0021 p:0164 s:0102 b:0099 l:000083 d:000098 BLOCK  c:/ruby19/lib/ruby/1.9.1/psych/visitors/to_ruby.rb:226
c:0020 p:---- s:0094 b:0094 l:000093 d:000093 FINISH
c:0019 p:---- s:0092 b:0092 l:000087 d:000091 IFUNC
c:0018 p:---- s:0090 b:0090 l:000089 d:000089 CFUNC  :each
c:0017 p:---- s:0088 b:0088 l:000087 d:000087 CFUNC  :each_slice
c:0016 p:0052 s:0084 b:0084 l:000083 d:000083 METHOD c:/ruby19/lib/ruby/1.9.1/psych/visitors/to_ruby.rb:211
c:0015 p:0091 s:0079 b:0079 l:000078 d:000078 METHOD c:/ruby19/lib/ruby/1.9.1/psych/visitors/to_ruby.rb:123
c:0014 p:0030 s:0065 b:0065 l:000064 d:000064 METHOD c:/ruby19/lib/ruby/1.9.1/psych/visitors/visitor.rb:15
c:0013 p:0013 s:0061 b:0061 l:000060 d:000060 METHOD c:/ruby19/lib/ruby/1.9.1/psych/visitors/visitor.rb:5
c:0012 p:0012 s:0057 b:0057 l:000056 d:000056 METHOD c:/ruby19/lib/ruby/1.9.1/psych/visitors/to_ruby.rb:16
c:0011 p:0026 s:0049 b:0049 l:000048 d:000048 METHOD c:/ruby19/lib/ruby/1.9.1/psych/nodes/node.rb:35
c:0010 p:0029 s:0046 b:0046 l:000045 d:000045 METHOD c:/ruby19/lib/ruby/1.9.1/psych.rb:113
c:0009 p:0080 s:0041 b:0041 l:000040 d:000040 METHOD c:/ruby19/lib/ruby/1.9.1/rubygems/config_file.rb:239
c:0008 p:0212 s:0037 b:0037 l:000036 d:000036 METHOD c:/ruby19/lib/ruby/1.9.1/rubygems/config_file.rb:179
c:0007 p:---- s:0028 b:0028 l:000027 d:000027 FINISH
c:0006 p:---- s:0026 b:0026 l:000025 d:000025 CFUNC  :new
c:0005 p:0022 s:0022 b:0021 l:000020 d:000020 METHOD c:/ruby19/lib/ruby/1.9.1/rubygems/gem_runner.rb:78
c:0004 p:0118 s:0017 b:0017 l:000016 d:000016 METHOD c:/ruby19/lib/ruby/1.9.1/rubygems/gem_runner.rb:51
c:0003 p:0164 s:0009 b:0009 l:0019bc d:0021a8 EVAL   c:/ruby19/bin/gem:21
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:0019bc d:0019bc TOP

-- Ruby level backtrace information ----------------------------------------
c:/ruby19/bin/gem:21:in <main>'
c:/ruby19/lib/ruby/1.9.1/rubygems/gem_runner.rb:51:inrun'
```

c:/ruby19/lib/ruby/1.9.1/rubygems/gem_runner.rb:78:in do_configuration'
c:/ruby19/lib/ruby/1.9.1/rubygems/gem_runner.rb:78:innew'
c:/ruby19/lib/ruby/1.9.1/rubygems/config_file.rb:179:in initialize'
c:/ruby19/lib/ruby/1.9.1/rubygems/config_file.rb:239:inload_file'
c:/ruby19/lib/ruby/1.9.1/psych.rb:113:in load'
c:/ruby19/lib/ruby/1.9.1/psych/nodes/node.rb:35:into_ruby'
c:/ruby19/lib/ruby/1.9.1/psych/visitors/to_ruby.rb:16:in accept'
c:/ruby19/lib/ruby/1.9.1/psych/visitors/visitor.rb:5:inaccept'
c:/ruby19/lib/ruby/1.9.1/psych/visitors/visitor.rb:15:in visit'
c:/ruby19/lib/ruby/1.9.1/psych/visitors/to_ruby.rb:123:invisit_Psych_Nodes_Mapping'
c:/ruby19/lib/ruby/1.9.1/psych/visitors/to_ruby.rb:211:in revive_hash'
c:/ruby19/lib/ruby/1.9.1/psych/visitors/to_ruby.rb:211:ineach_slice'
c:/ruby19/lib/ruby/1.9.1/psych/visitors/to_ruby.rb:211:in each'
c:/ruby19/lib/ruby/1.9.1/psych/visitors/to_ruby.rb:226:inblock in revive_hash'
c:/ruby19/lib/ruby/1.9.1/psych/visitors/to_ruby.rb:16:in accept'
c:/ruby19/lib/ruby/1.9.1/psych/visitors/visitor.rb:5:inaccept'
c:/ruby19/lib/ruby/1.9.1/psych/visitors/visitor.rb:15:in visit'
c:/ruby19/lib/ruby/1.9.1/psych/visitors/to_ruby.rb:46:invisit_Psych_Nodes_Scalar'
c:/ruby19/lib/ruby/1.9.1/psych/scalar_scanner.rb:71:in tokenize'
c:/ruby19/lib/ruby/1.9.1/psych/scalar_scanner.rb:71:inInteger'

-- C level backtrace information ---
C:\WINDOWS\system32\ntdll.dll(KiFastSystemCallRet+0x0) [0x7c90e514]
C:\WINDOWS\system32\kernel32.dll(WaitForSingleObject+0x12) [0x7c802542]

-- Other runtime information ---

- Loaded script: c:/ruby19/bin/gem

- Loaded features:

  0 enumerator.so
  1 c:/ruby19/lib/ruby/1.9.1/i386-mingw32/enc/encdb.so
  2 c:/ruby19/lib/ruby/1.9.1/i386-mingw32/enc/iso_8859_1.so
  3 c:/ruby19/lib/ruby/1.9.1/i386-mingw32/enc/trans/transdb.so
  4 c:/ruby19/lib/ruby/1.9.1/rubygems/defaults.rb
  5 c:/ruby19/lib/ruby/1.9.1/i386-mingw32/rbconfig.rb
  6 c:/ruby19/lib/ruby/1.9.1/rubygems/deprecate.rb
  7 c:/ruby19/lib/ruby/1.9.1/rubygems/exceptions.rb
  8 c:/ruby19/lib/ruby/1.9.1/rubygems/defaults/operating_system.rb
  9 c:/ruby19/lib/ruby/1.9.1/rubygems/custom_require.rb
  10 c:/ruby19/lib/ruby/1.9.1/rubygems.rb
  11 c:/ruby19/lib/ruby/1.9.1/optparse.rb
  12 c:/ruby19/lib/ruby/1.9.1/rubygems/user_interaction.rb
  13 c:/ruby19/lib/ruby/1.9.1/rubygems/command.rb
  14 c:/ruby19/lib/ruby/1.9.1/rubygems/command_manager.rb
  15 c:/ruby19/lib/ruby/1.9.1/i386-mingw32/etc.so
  16 c:/ruby19/lib/ruby/1.9.1/i386-mingw32/enc/utf_16le.so
  17 c:/ruby19/lib/ruby/1.9.1/i386-mingw32/enc/trans/utf_16_32.so
  18 c:/ruby19/lib/ruby/1.9.1/i386-mingw32/enc/trans/single_byte.so
  19 c:/ruby19/lib/ruby/1.9.1/rubygems/config_file.rb
  20 c:/ruby19/lib/ruby/1.9.1/rubygems/doc_manager.rb
  21 c:/ruby19/lib/ruby/1.9.1/rubygems/version.rb
  22 c:/ruby19/lib/ruby/1.9.1/rubygems/requirement.rb
  23 c:/ruby19/lib/ruby/1.9.1/rubygems/platform.rb
  24 c:/ruby19/lib/ruby/1.9.1/rubygems/specification.rb
  25 c:/ruby19/lib/ruby/1.9.1/rubygems/path_support.rb
  26 c:/ruby19/lib/ruby/1.9.1/rubygems/dependency.rb
  27 c:/ruby19/lib/ruby/gems/1.9.1/gems/yard-0.7.2/lib/yard/rubygems/specification.rb
  28 c:/ruby19/lib/ruby/gems/1.9.1/gems/yard-0.7.2/lib/yard/rubygems/doc_manager.rb
  29 c:/ruby19/lib/ruby/1.9.1/rubygems/gem_runner.rb
  30 c:/ruby19/lib/ruby/1.9.1/i386-mingw32/psych.so
  31 c:/ruby19/lib/ruby/1.9.1/i386-mingw32/stringio.so
  32 c:/ruby19/lib/ruby/1.9.1/psych/nodes/node.rb
  33 c:/ruby19/lib/ruby/1.9.1/psych/nodes/stream.rb
  34 c:/ruby19/lib/ruby/1.9.1/psych/nodes/document.rb
  35 c:/ruby19/lib/ruby/1.9.1/psych/nodes/sequence.rb

```
36 c:/ruby19/lib/ruby/1.9.1/psych/nodes/scalar.rb
37 c:/ruby19/lib/ruby/1.9.1/psych/nodes/mapping.rb
38 c:/ruby19/lib/ruby/1.9.1/psych/nodes/alias.rb
39 c:/ruby19/lib/ruby/1.9.1/psych/nodes.rb
40 c:/ruby19/lib/ruby/1.9.1/psych/streaming.rb
41 c:/ruby19/lib/ruby/1.9.1/psych/visitors/visitor.rb
42 c:/ruby19/lib/ruby/1.9.1/i386-mingw32/strscan.so
43 c:/ruby19/lib/ruby/1.9.1/psych/scalar_scanner.rb
44 c:/ruby19/lib/ruby/1.9.1/psych/visitors/to_ruby.rb
45 c:/ruby19/lib/ruby/1.9.1/psych/visitors/emitter.rb
46 c:/ruby19/lib/ruby/1.9.1/psych/visitors/yaml_tree.rb
47 c:/ruby19/lib/ruby/1.9.1/psych/json/ruby_events.rb
48 c:/ruby19/lib/ruby/1.9.1/psych/visitors/json_tree.rb
49 c:/ruby19/lib/ruby/1.9.1/psych/visitors/depth_first.rb
50 c:/ruby19/lib/ruby/1.9.1/psych/visitors.rb
51 c:/ruby19/lib/ruby/1.9.1/psych/handler.rb
52 c:/ruby19/lib/ruby/1.9.1/psych/tree_builder.rb
53 c:/ruby19/lib/ruby/1.9.1/psych/parser.rb
54 c:/ruby19/lib/ruby/1.9.1/psych/omap.rb
55 c:/ruby19/lib/ruby/1.9.1/psych/set.rb
56 c:/ruby19/lib/ruby/1.9.1/psych/coder.rb
57 c:/ruby19/lib/ruby/1.9.1/psych/core_ext.rb
58 c:/ruby19/lib/ruby/1.9.1/i386-mingw32/date_core.so
59 c:/ruby19/lib/ruby/1.9.1/date/format.rb
60 c:/ruby19/lib/ruby/1.9.1/date.rb
61 c:/ruby19/lib/ruby/1.9.1/psych/deprecated.rb
62 c:/ruby19/lib/ruby/1.9.1/psych/json.rb
63 c:/ruby19/lib/ruby/1.9.1/psych.rb
64 c:/ruby19/lib/ruby/1.9.1/yaml.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.

C:>gdb --args ruby -S gem --version
GNU gdb (GDB) 7.3
Copyright (C) 2011 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 "mingw32".
For bug reporting instructions, please see:
http://www.gnu.org/software/gdb/bugs/...
Reading symbols from c:\ruby19\bin\ruby.exe...done.
(gdb) run
Starting program: c:\ruby19\bin\ruby.exe -S gem --version
[New Thread 1480.0x974]
[New Thread 1480.0x680]

Program received signal SIGSEGV, Segmentation fault.
0x77c3554a in msvcrt!_abnormal_termination ()
from C:\WINDOWS\system32\msvcrt.dll
(gdb) bt
#0  0x77c3554a in msvcrt!_abnormal_termination ()
from C:\WINDOWS\system32\msvcrt.dll
#1  0x77c39bc6 in strerror () from C:\WINDOWS\system32\msvcrt.dll
Backtrace stopped: previous frame inner to this frame (corrupt stack?)
(gdb) thread
Current thread is 1 (Thread 1480.0x974) info threads
Id   Target Id         Frame
2    Thread 1480.0x680 0x7c90e514 in ntdll!LdrAccessResource ()
```

from C:\WINDOWS\system32\ntdll.dll

- 1 Thread 1480.0x974 0x77c3554a in msvcrt!_abnormal_termination () from C:\WINDOWS\system32\msvcrt.dll (gdb)

Related issues:

Related to Backport193 - Backport #5518: Please backport r33577 (mingw: appen...	**Closed**	**10/31/2011**
Has duplicate Ruby trunk - Bug #5407: Cannot build ruby-1.9.3-rc1 with TDM-GC...	**Closed**	**10/05/2011**

History

#1 - 09/28/2011 09:13 AM - naruse (Yui NARUSE)

- Status changed from Open to Assigned

- Assignee set to luislavena (Luis Lavena)

#2 - 09/28/2011 11:12 AM - usa (Usaku NAKAMURA)

FYI:
I can't reproduce on i386-mswin32 @ 1.9.3dev r33323 (=1.9.3-rc1).

The only difference between r33323 and r33347 is a patch about ext/openssl, so I guess it's not the cause.

#3 - 09/28/2011 10:51 PM - jonforums (Jon Forums)

Aaron...would you quickly look at this as the segfault happens in psych's scalar_scanner.rb after running through some of psych's handling for rubygems/config_file.rb?

C:>gem --version
c:/ruby19/lib/ruby/1.9.1/psych/scalar_scanner.rb:71: [BUG] Segmentation fault

Later I plan to test some specific psych code on simpler .gemrc files to see if that leads anywhere as I really only need the gem: --no-ri --no-rdoc. FYI the current %USERPROFILE%/.gemrc (CRLF delimited) on the failing machines is

---

:backtrace: false
:benchmark: false
:bulk_threshold: 1000
:sources:

- http://rubygems.org :update_sources: true :verbose: true gem: --no-ri --no-rdoc

'wrong code' bug reports like http://gcc.gnu.org/bugzilla/show_bug.cgi?id=49140 also concern me.

#4 - 09/28/2011 11:23 PM - jonforums (Jon Forums)

simple .gemrc is a red herring...still segfaults in the same way with only

gem: --no-ri --no-rdoc

#5 - 09/28/2011 11:47 PM - luislavena (Luis Lavena)

Jon Forums wrote:

> Aaron...would you quickly look at this as the segfault happens in psych's scalar_scanner.rb after running through some of psych's handling for rubygems/config_file.rb?
>
> C:>gem --version
> c:/ruby19/lib/ruby/1.9.1/psych/scalar_scanner.rb:71: [BUG] Segmentation fault
>
> Later I plan to test some specific psych code on simpler .gemrc files to see if that leads anywhere as I really only need the gem: --no-ri --no-rdoc. FYI the current %USERPROFILE%/.gemrc (CRLF delimited) on the failing machines is

Can rename %USERPROFILE%/.gem directory and try again?

Seems to me some gemspec is causing this. I'm trying to reproduce right now and will let you know.

#6 - 09/29/2011 12:05 AM - jonforums (Jon Forums)

Luis Lavena wrote:

> Jon Forums wrote:
>
> > Aaron...would you quickly look at this as the segfault happens in psych's scalar_scanner.rb after running through some of psych's handling for rubygems/config_file.rb?
> >
> > C:>gem --version
> > c:/ruby19/lib/ruby/1.9.1/psych/scalar_scanner.rb:71: [BUG] Segmentation fault
> >
> > Later I plan to test some specific psych code on simpler .gemrc files to see if that leads anywhere as I really only need the gem: --no-ri --no-rdoc. FYI the current %USERPROFILE%/.gemrc (CRLF delimited) on the failing machines is
>
> Can rename %USERPROFILE%/.gem directory and try again?
>
> Seems to me some gemspec is causing this. I'm trying to reproduce right now and will let you know.

renamed to %USERPROFILE%/.badg and I still see the segfault.

tried again after deleting .badg to the Recycle Bin and saw the same thing.

#7 - 09/29/2011 12:56 AM - jonforums (Jon Forums)

OK, plain vanilla 1.9.3 RubyInstaller build with no additional gems, no .gem, a clean PATH, and using psych to load the simple .gemrc.

Same segfault and gdb results.

```
C:\Documents and Settings\Jon>echo %PATH%
C:\rbtst\bin;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem

C:\Documents and Settings\Jon>ruby --version
ruby 1.9.3dev (2011-09-27 revision 33347) [i386-mingw32]

C:\Documents and Settings\Jon>dir .gem*
Volume in drive C has no label.
Volume Serial Number is D448-9EA3

Directory of C:\Documents and Settings\Jon

09/28/2011  10:22 AM                24 .gemrc
1 File(s)             24 bytes
0 Dir(s)  16,150,208,512 bytes free

C:\Documents and Settings\Jon>type .gemrc
gem: --no-ri --no-rdoc

C:\Documents and Settings\Jon>type qt.rb
require 'psych'
require 'yaml'
YAML.load_file('.gemrc')

C:\Documents and Settings\Jon>ruby qt.rb
C:/rbtst/lib/ruby/1.9.1/psych/scalar_scanner.rb:71: [BUG] Segmentation fault
ruby 1.9.3dev (2011-09-27 revision 33347) [i386-mingw32]
...
```

#8 - 09/29/2011 01:24 AM - jonforums (Jon Forums)

uh-oh...

going to try a build using the previous v0.1.3 libyaml instead of the current 0.1.4.

```
C:\Documents and Settings\Jon>irb
irb(main):001:0> require 'syck'
=> true
irb(main):002:0> require 'yaml'
=> true
irb(main):003:0> YAML.load_file('.gemrc')
=> {"gem"=>"--no-ri --no-rdoc"}
```

#9 - 09/29/2011 04:53 AM - luislavena (Luis Lavena)

- Status changed from Assigned to Feedback

Jon, I can't reproduce:

```
V:>ruby -rpsych -ryaml -ve "puts Psych::LIBYAML_VERSION; puts YAML.load(\"gem: --no-ri --no-rdoc\r\n\")"
ruby 1.9.3dev (2011-09-27 revision 33347) [i386-mingw32]
0.1.4
{"gem"=>"--no-ri --no-rdoc"}
```

I've also tested with YAML.load_file:

```
V:>type .gemrc
gem: --no-ri --no-rdoc

V:>ruby -rpsych -ryaml -ve "puts YAML.load_file('.gemrc')"
ruby 1.9.3dev (2011-09-27 revision 33347) [i386-mingw32]
{"gem"=>"--no-ri --no-rdoc"}
```

This was tested with:

- Windows 7 Ultimate x64
- TDM-GCC 4.5.2
- TDM-GCC 4.6.1

Booting a Windows XP SP2 VM as we speak to test out more closely to your environment.

#10 - 09/29/2011 05:04 AM - jonforums (Jon Forums)

Luis...no repro, hmm, but good you're not seeing it with either of 4.5.2 or 4.6.1.

Reverting to libyaml v0.1.3 still segfaults in the same way for me.

```
C:\Documents and Settings\Jon>echo %PATH%
c:\rbtst\bin;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem

C:\Documents and Settings\Jon>ruby -rpsych -ryaml -e "puts YAML::LIBYAML_VERSION; YAML.load_file('.gemrc')
0.1.3
c:/rbtst/lib/ruby/1.9.1/psych/scalar_scanner.rb:71: [BUG] Segmentation fault
ruby 1.9.3dev (2011-09-27 revision 33347) [i386-mingw32]
...

C:\Documents and Settings\Jon>ruby -rsyck -ryaml -e "puts Syck::VERSION; puts YAML.load_file('.gemrc')
0.60
{"gem"=>"--no-ri --no-rdoc"}
```

#11 - 09/29/2011 10:51 PM - jonforums (Jon Forums)

Luis...were you able to repro on your XP SP2 VM running on Win7 Ultimate 64bit?

#12 - 10/01/2011 11:21 AM - luislavena (Luis Lavena)

- Status changed from Feedback to Assigned

Sorry for the delay, too much work.

I was able to reproduce the issue under Windows XP SP2

The last point that can be traced appears to be rb_longjmp with TAG_RAISE when attempt to raise rb_eArgError.

Tried to debug using GDB without success.

I'll try 4.5.2 and 4.6.2 (mingw-w64) next.

#13 - 10/01/2011 01:50 PM - jojelino (jojelino _)

i had same issue before although it maybe not same one.
The location of error triggered was msvcrt!_abnormal_termination.
From gcc 4.6, ABI has changed so %esp can be invalid memory reference. so msvcrt!longjmp sigsegvs in this case. it has NLG_Notify which not only have no use but also make sigsegv.
Problem will persist until mingw32 implement/link alternative setjmp/longjmp.

there are two of way to fix this.

1. it is known that mingw64 implemented alternative setjmp/longjmp so you can use i686-pc-mingw64-gcc to build ruby so that we avoid sigsegv for this occasion.
2. make ruby call setjmp/longjmp which doesn't sigsegv.

tdm-gcc is built with mingw32. so i think it would be related.

#14 - 10/01/2011 11:31 PM - luislavena (Luis Lavena)

Independent of being mingw or mingw-w64 provided version of GCC, 4.6.x seems to segfault too.

I've tried mingw-w64 GCC 4.6.2 with same result.

Downgrade to libyaml 0.1.3 did not help. Comment from jojelino (jojelino _) seems to have some good information.

Usaku NAKAMURA, if you can't reproduce with mswin then the issue is not in Ruby but the compiler itself.

Will investigate further but any comment or suggestion you have please let me know.

#15 - 10/02/2011 05:17 AM - jonforums (Jon Forums)

jojelino _ wrote:

> i had same issue before although it maybe not same one.
> The location of error triggered was msvcrt!_abnormal_termination.
> From gcc 4.6, ABI has changed so %esp can be invalid memory reference. so msvcrt!longjmp sigsegvs in this case. it has NLG_Notify which not only have no use but also make sigsegv.
> Problem will persist until mingw32 implement/link alternative setjmp/longjmp.
>
> there are two of way to fix this.
>
> 1. it is known that mingw64 implemented alternative setjmp/longjmp so you can use i686-pc-mingw64-gcc to build ruby so that we avoid sigsegv for this occasion.
> 2. make ruby call setjmp/longjmp which doesn't sigsegv.
>
> tdm-gcc is built with mingw32. so i think it would be related.

@jojelino...thanks for the info and I just found your post

http://www.mail-archive.com/gcc-bugs@gcc.gnu.org/msg332206.html

Any thoughts on why the segfault on WinXP but not Win7?

UPDATE: just read Kai's comment

http://www.mail-archive.com/gcc-bugs@gcc.gnu.org/msg332254.html

but Kai's comment (mingw.org header handling for setjmp) doesn't sync with Luis' results in which he saw the segfault with mingw-w64 GCC 4.6.2

#16 - 10/02/2011 09:37 AM - luislavena (Luis Lavena)

- Assignee changed from luislavena (Luis Lavena) to nobu (Nobuyoshi Nakada)

Nobu-san, any suggestion?

#17 - 10/04/2011 07:50 PM - jojelino (jojelino _)

Luis Lavena wrote:

> Independent of being mingw or mingw-w64 provided version of GCC, 4.6.x seems to segfault too.
>
> I've tried mingw-w64 GCC 4.6.2 with same result.

In fact, i had sigsegv in mingw-w64 too. the problem came from msvcrt!longjmp dereferences ebp+8 which maybe invalid one. now i can remind that mingw-w64 didn't implement alternative setjmp/longjmp. I'm sorry for that. So, adding hidden argument to longjmp prototype didn't help(it just ensures that esp+8 has valid reference. the problem remains) i recommend you to use alternative longjmp/setjmp implementation from other open source projects.(such as reactos, wine, deloie's implementation... or if you are brave, try linking with msvcrt[9-10].dll which doesn't dereferences ebp+8 in NLG_Notify. even though i didn't.)

#18 - 10/05/2011 06:17 AM - luislavena (Luis Lavena)

- Status changed from Assigned to Feedback

- Assignee changed from nobu (Nobuyoshi Nakada) to tenderlovemaking (Aaron Patterson)

jon (Jonas Jasas):

Just tested trunk at r33401 with GCC 4.6.1 (TDM-1) under Windows XP SP2 and worked without segfaulting:

V:>ver

Microsoft Windows XP [Versión 5.1.2600]

V:>ruby -rpsych -ve "puts Psych.load(\"gem: --no-ri --no-rdoc\r\n\")"
ruby 1.9.4dev (2011-10-05) [i386-mingw32]
{"gem"=>"--no-ri --no-rdoc"}

This commit and the following (r33403 and r33404) should be backported to 1.9.3

Assigning to Aaron Patterson so he can confirm if this is correct.

#19 - 10/05/2011 06:31 AM - jonforums (Jon Forums)

luis (Luis Lopez), excellent; thank you. I'll confirm your results by testing on my two native WinXP SP3 boxes tomorrow.

#20 - 10/06/2011 01:35 AM - jonforums (Jon Forums)

trunk versions built with 4.6.1 running under WinXP SP3 consistently work for me.

It's only the ruby_1_9_3 branch built (just tried r33347) with either TDM-GCC 4.6.1 or plain vanilla mingw.org GCC 4.6.1 that segfault on my WinXP SP3 machines.

I'll test again as soon as I see the latest trunk Psych commits backported to 1.9.3. Time permitting I'll try to track back from scalar_scanner.rb and see if it leads to a setjmp/longjump as jojelino (jojelino _) shared. Aaron may know right away, or if we're lucky, may have already routed around the issue in trunk.

#21 - 10/06/2011 10:28 AM - usa (Usaku NAKAMURA)

Luis, sorry for my late reply.
My tested environment doesn't have libyaml.
Probably it's the reason why I couldn't reproduce this problem.

#22 - 10/06/2011 11:51 AM - luislavena (Luis Lavena)

- Assignee changed from tenderlovemaking (Aaron Patterson) to luislavena (Luis Lavena)

Usaku NAKAMURA wrote:

> Luis, sorry for my late reply.
> My tested environment doesn't have libyaml.
> Probably it's the reason why I couldn't reproduce this problem.

Recent change in trunk related to Psych and the way exceptions are rescued seems to be the cause of the issue.

This seems to have an effect on setjmp/longjmp implementation under GCC 4.6 and Windows XP.

Going to manually backport r33401 over ruby_1_9_3 and test it (to my bad it takes time and I'm less than 8 hours to take a flight)

Will keep you guys posted.

#23 - 10/07/2011 01:06 AM - jonforums (Jon Forums)

> Going to manually backport r33401 over ruby_1_9_3 and test it...

May need more than r33401.

After running git co ruby_1_9_3 && git cherry-pick -n b7c66e3 and cleaning the conflicts, the build completed, make test passed, make test-all TESTS=psych failed 58 times, and I got a different segfault from scalar_scannar.rb.

But I may have mangled the de-conflict. Will look again after today's meetings.

#24 - 10/15/2011 09:55 PM - luislavena (Luis Lavena)

- Assignee changed from luislavena (Luis Lavena) to nobu (Nobuyoshi Nakada)

- Priority changed from Normal to 6

Hello,

This seems to be a regression of the VM perhaps? Using same compiler (GCC 4.6.1) but against trunk, it works perfectly:

V:>ruby -v

ruby 1.9.4dev (2011-10-14 trunk 33469) [i386-mingw32]

V:>ruby -rpsych -ve "puts Psych.load(\"gem: --no-ri --no-rdoc\r\n\")"
ruby 1.9.4dev (2011-10-14 trunk 33469) [i386-mingw32]
{"gem"=>"--no-ri --no-rdoc"}

The changes around rescuing the exceptions from Integer or Float seems not to be the issue but the way longjmp and setjmp works.

Did something change that I'm missing?

This is a blocker to release Ruby 1.9.3, as mentioned over the maintainers email exchange.

#25 - 10/23/2011 06:37 AM - luislavena (Luis Lavena)

- Status changed from Feedback to Closed

- Assignee changed from nobu (Nobuyoshi Nakada) to luislavena (Luis Lavena)

Closing it out as duplicate of #5407 as efforts on solve the issue has been made in that issue.

Thank you.