

Ruby trunk - Bug #15223

Windows 1809 Update causes almost all file operations to segfault

10/12/2018 03:01 AM - eliza (Eliza Velasquez)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	2.3.7, 2.5.1	Backport: 2.3: DONE, 2.4: DONE, 2.5: DONE
Description		
File I/O has almost completely broken after the recent Windows 1809 update when compiling Ruby against MSVCRT.		
Here is the relevant output when compiling Ruby 2.3.7 with Visual Studio 2017 Community, toolset v141, x64. The stacktrace for 2.3.7 was more detailed than 2.5.1, but the error appears in both at apparently the same locations in win32.c.		
<pre>linking miniruby.exe ruby 2.3.7p456 (2018-03-28 revision 63024) [x64-mswin64_140] generating encdb.h generating enc.mk ./enc/make_encmake.rb:10: [BUG] Segmentation fault ruby 2.3.7p456 (2018-03-28 revision 63024) [x64-mswin64_140] -- Control frame information ----- c:0003 p:---- s:0016 e:000015 CFUNC :require c:0002 p:0091 s:0012 E:000780 EVAL ./enc/make_encmake.rb:10 [FINISH] c:0001 p:0000 s:0002 E:0016b0 (none) [FINISH] -- Ruby level backtrace information ----- ./enc/make_encmake.rb:10:in `<main>' ./enc/make_encmake.rb:10:in `require' -- C level backtrace information ----- C:\WINDOWS\SYSTEM32\ntdll.dll (ZwWaitForSingleObject+0x14) [0x00007FF904CBE614] C:\WINDOWS\System32\KERNELBASE.dll (WaitForSingleObjectEx+0x93) [0x00007FF900FE4313] C:\Users\Eliza\Projects\ruby\miniruby.exe (rb_print_backtrace+0x34) [0x00007FF6594AF514] c:\users\eliza\projects\ruby\vm_dump.c:743 C:\Users\Eliza\Projects\ruby\miniruby.exe (rb_vm_bugreport+0x7d) [0x00007FF6594AF599] c:\users\eliza\projects\ruby\vm_dump.c:1036 C:\Users\Eliza\Projects\ruby\miniruby.exe (rb_bug_context+0x60) [0x00007FF6593CE0BC] c:\users\eliza\projects\ruby\error.c:435 C:\Users\Eliza\Projects\ruby\miniruby.exe (sigsegv+0x2a) [0x00007FF65945428A] c:\users\eliza\projects\ruby\signal.c:890 C:\WINDOWS\System32\ucrtbase.dll (seh_filter_exe+0x233) [0x00007FF901B5D713] C:\Users\Eliza\Projects\ruby\miniruby.exe (`__srt_common_main_seh':`1'::filt\$0+0x16) [0x00007FF6594C8EDE] f:\dd\vctools\crt\vcstartup\src\startup\exe_common.inl:304 C:\WINDOWS\SYSTEM32\VCRUNTIME140.dll (_C_specific_handler+0xa0) [0x00007FF8F8BEBF10] C:\WINDOWS\SYSTEM32\ntdll.dll (_chkstk+0x11f) [0x00007FF904CC35AF] C:\WINDOWS\SYSTEM32\ntdll.dll (RtlWalkFrameChain+0x14bf) [0x00007FF904C24AAF] C:\WINDOWS\SYSTEM32\ntdll.dll (KiUserExceptionDispatcher+0x2e) [0x00007FF904CC231E] C:\WINDOWS\SYSTEM32\ntdll.dll (RtlExpandEnvironmentStrings+0x20b) [0x00007FF904C3982B] C:\WINDOWS\SYSTEM32\ntdll.dll (RtlEnterCriticalSection+0x12c) [0x00007FF904C35FDC] C:\WINDOWS\SYSTEM32\ntdll.dll (RtlEnterCriticalSection+0x40) [0x00007FF904C35EF0] C:\Users\Eliza\Projects\ruby\miniruby.exe (rb_w32_read+0xd3) [0x00007FF6594C18DB] c:\users\eliza\projects\ruby\win32\win32.c:6914 C:\Users\Eliza\Projects\ruby\miniruby.exe (rb_thread_io_blocking_region+0x10a) [0x00007FF6594B6446] c:\users\eliza\projects\ruby\thread.c:1430 C:\Users\Eliza\Projects\ruby\miniruby.exe (io_fillbuf+0x7e) [0x00007FF6593F367A] c:\users\eliza\projects\ruby\io.c:1770 C:\Users\Eliza\Projects\ruby\miniruby.exe (rb_io_getline_fast+0x12b) [0x00007FF6593F9137] c:\users\eliza\projects\ruby\io.c:3023 C:\Users\Eliza\Projects\ruby\miniruby.exe (rb_io_getline_1+0x14e) [0x00007FF6593F8C72] c:\users\eliza\projects\ruby\io.c:3106</pre>		

```

C:\Users\Eliza\Projects\ruby\miniruby.exe (parser_nextc+0x52) [0x00007FF65941C4CA] c:\users\eliza\p
rojects\ruby\parse.y:5800
C:\Users\Eliza\Projects\ruby\miniruby.exe (yycompile0+0x18e) [0x00007FF659425DD2] c:\users\eliza\pr
ojects\ruby\parse.y:5559
C:\Users\Eliza\Projects\ruby\miniruby.exe (rb_suppress_tracing+0x116) [0x00007FF6594B19C2] c:\users
\eliza\projects\ruby\vm_trace.c:407
C:\Users\Eliza\Projects\ruby\miniruby.exe (rb_parser_compile_file_path+0x74) [0x00007FF65941FC20] c
:\users\eliza\projects\ruby\parse.y:5738
C:\Users\Eliza\Projects\ruby\miniruby.exe (load_file_internal+0x3e5) [0x00007FF6594507E1] c:\users\
eliza\projects\ruby\ruby.c:1776
C:\Users\Eliza\Projects\ruby\miniruby.exe (rb_ensure+0xc8) [0x00007FF6593D0998] c:\users\eliza\proj
ects\ruby\eval.c:938
C:\Users\Eliza\Projects\ruby\miniruby.exe (load_file+0x10b) [0x00007FF6594503A7] c:\users\eliza\pro
jects\ruby\ruby.c:1897
C:\Users\Eliza\Projects\ruby\miniruby.exe (rb_load_file_str+0x45) [0x00007FF659452551] c:\users\eli
za\projects\ruby\ruby.c:1912
C:\Users\Eliza\Projects\ruby\miniruby.exe (rb_load_internal0+0x10b) [0x00007FF6593D458F] c:\users\e
liza\projects\ruby\load.c:616
C:\Users\Eliza\Projects\ruby\miniruby.exe (rb_require_internal+0x2cd) [0x00007FF6593D4ACD] c:\users
\eliza\projects\ruby\load.c:1000
C:\Users\Eliza\Projects\ruby\miniruby.exe (rb_require_safe+0xe) [0x00007FF6593D4B7E] c:\users\eliza
\projects\ruby\load.c:1047
C:\Users\Eliza\Projects\ruby\miniruby.exe (vm_call_cfunc_with_frame+0x122) [0x00007FF6594A6B96] c:\
users\eliza\projects\ruby\vm_inshelper.c:1644
C:\Users\Eliza\Projects\ruby\miniruby.exe (vm_call_method_each_type+0x3f8) [0x00007FF6594A75A0] c:\
users\eliza\projects\ruby\vm_inshelper.c:2026
C:\Users\Eliza\Projects\ruby\miniruby.exe (vm_call_method+0xfb) [0x00007FF6594A716F] c:\users\eliza
\projects\ruby\vm_inshelper.c:2189
C:\Users\Eliza\Projects\ruby\miniruby.exe (vm_exec_core+0xcde) [0x00007FF6594A9B22] c:\users\eliza\
projects\ruby\vm_exec.c:118
C:\Users\Eliza\Projects\ruby\miniruby.exe (vm_exec+0xb3) [0x00007FF6594A88D7] c:\users\eliza\projec
ts\ruby\vm.c:1694
C:\Users\Eliza\Projects\ruby\miniruby.exe (ruby_exec_internal+0xc1) [0x00007FF6593D2635] c:\users\e
liza\projects\ruby\eval.c:248
C:\Users\Eliza\Projects\ruby\miniruby.exe (ruby_exec_node+0x1d) [0x00007FF6593D268D] c:\users\eliza
\projects\ruby\eval.c:311
C:\Users\Eliza\Projects\ruby\miniruby.exe (ruby_run_node+0x30) [0x00007FF6593D28EC] c:\users\eliza\
projects\ruby\eval.c:302
C:\Users\Eliza\Projects\ruby\miniruby.exe (main+0x40) [0x00007FF6593A1040] c:\users\eliza\projects\
ruby\main.c:38
C:\Users\Eliza\Projects\ruby\miniruby.exe (__scrt_common_main_seh+0x10c) [0x00007FF6594C8594] f:\dd
\vc\tools\crt\vcstartup\src\startup\exe_common.inl:288
C:\WINDOWS\System32\KERNEL32.DLL (BaseThreadInitThunk+0x14) [0x00007FF902AB7E94]

```

-- Other runtime information -----

* Loaded script: ./enc/make_encmake.rb

* Loaded features:

- 0 enumerator.so
- 1 thread.rb
- 2 rational.so
- 3 complex.so
- 4 mkmf.rb
- 5 C:/Users/Eliza/Projects/ruby/rbconfig.rb
- 6 C:/Users/Eliza/Projects/ruby/lib/fileutils.rb
- 7 C:/Users/Eliza/Projects/ruby/lib/shellwords.rb

Switching out the Ruby version for 2.5.1, the compiler toolset for v140, or the architecture for x86 had no effect. If Ruby is successfully built on another Windows system without the update and copied to an affected system, ruby.exe will crash. The output for me was as follows:

```

C:/Users/Eliza/.conan/data/ruby/2.3.7/eliza/stable/package/5d98350dbfede072d5a445d3f1d53ef8d94f28c
e/lib/ruby/2.3.0/irb/locale.rb:130:in `read': Bad file descriptor @ io_fread - C:/Users/Eliza/.con
an/data/ruby/2.3.7/eliza/stable/package/5d98350dbfede072d5a445d3f1d53ef8d94f28ce/lib/ruby/2.3.0/ir
b/lc/error.rb (Errno::EBADF)

```

```
from C:/Users/Eliza/.conan/data/ruby/2.3.7/eliza/stable/package/5d98350dbfede072d5a445d3f1
d53ef8d94f28ce/lib/ruby/2.3.0/irb/locale.rb:130:in `block in real_load'
from C:/Users/Eliza/.conan/data/ruby/2.3.7/eliza/stable/package/5d98350dbfede072d5a445d3f1
d53ef8d94f28ce/lib/ruby/2.3.0/irb/magic-file.rb:19:in `open'
from C:/Users/Eliza/.conan/data/ruby/2.3.7/eliza/stable/package/5d98350dbfede072d5a445d3f1
d53ef8d94f28ce/lib/ruby/2.3.0/irb/locale.rb:130:in `real_load'
from C:/Users/Eliza/.conan/data/ruby/2.3.7/eliza/stable/package/5d98350dbfede072d5a445d3f1
d53ef8d94f28ce/lib/ruby/2.3.0/irb/locale.rb:110:in `load'
from C:/Users/Eliza/.conan/data/ruby/2.3.7/eliza/stable/package/5d98350dbfede072d5a445d3f1
d53ef8d94f28ce/lib/ruby/2.3.0/irb/init.rb:121:in `init_error'
from C:/Users/Eliza/.conan/data/ruby/2.3.7/eliza/stable/package/5d98350dbfede072d5a445d3f1
d53ef8d94f28ce/lib/ruby/2.3.0/irb/init.rb:18:in `setup'
from C:/Users/Eliza/.conan/data/ruby/2.3.7/eliza/stable/package/5d98350dbfede072d5a445d3f1
d53ef8d94f28ce/lib/ruby/2.3.0/irb.rb:378:in `start'
from C:/Users/Eliza/.conan/data/ruby/2.3.7/eliza/stable/package/5d98350dbfede072d5a445d3f1
d53ef8d94f28ce/bin/irb.cmd:19:in `<main>'
```

Linking to libruby also results in similar crashing behavior when attempting apparently any file operation.

At the time I'm writing this, in order to actually get the 1809 update in order to reproduce this behavior, joining the Windows insider program is required. I can try to provide more details if necessary.

Associated revisions

Revision 64913 - 10/04/2018 06:29 AM - usa (Usaku NAKAMURA)

Support ubasecrt.dll 10.0.17763.1 included in Windows 10 October 2018 Update

Revision 0b1e97d5 - 10/16/2018 11:23 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 64913: [Backport #15223]

Support ubasecrt.dll 10.0.17763.1 included in Windows 10 October 2018 Update

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_5@65100 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 65100 - 10/16/2018 11:23 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 64913: [Backport #15223]

Support ubasecrt.dll 10.0.17763.1 included in Windows 10 October 2018 Update

Revision bfdc70f8 - 10/17/2018 08:11 AM - usa (Usaku NAKAMURA)

merge revision(s) 64913: [Backport #15223]

Support ubasecrt.dll 10.0.17763.1 included in Windows 10 October 2018 Update

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_4@65110 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 65110 - 10/17/2018 08:11 AM - usa (Usaku NAKAMURA)

merge revision(s) 64913: [Backport #15223]

Support ubasecrt.dll 10.0.17763.1 included in Windows 10 October 2018 Update

Revision f5767da6 - 10/17/2018 09:46 AM - usa (Usaku NAKAMURA)

merge revision(s) 64913: [Backport #15223]

Support ubasecrt.dll 10.0.17763.1 included in Windows 10 October 2018 Update

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@65119 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 65119 - 10/17/2018 09:46 AM - usa (Usaku NAKAMURA)

merge revision(s) 64913: [Backport #15223]

Support ubasecrt.dll 10.0.17763.1 included in Windows 10 October 2018 Update

History

#1 - 10/12/2018 04:04 AM - shyouhei (Shyouhei Urabe)

- Status changed from Open to Feedback

This is supposedly fixed in revision [r64913](#). Can you try the latest trunk?

#2 - 10/12/2018 08:40 AM - naruse (Yui NARUSE)

As an another workaround and as far as I tried, Ruby binary compiled with Visual Studio v15 can work on Windows 1809 Update.

#3 - 10/13/2018 06:56 PM - eliza (Eliza Velasquez)

shyouhei (Shyouhei Urabe) wrote:

This is supposedly fixed in revision [r64913](#). Can you try the latest trunk?

Yes, this seems like it works. Thank you for your help.

#4 - 10/16/2018 07:15 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: UNKNOWN to 2.3: REQUIRED, 2.4: REQUIRED, 2.5: REQUIRED

- Status changed from Feedback to Closed

I believe [r64913](#) should be backported into stable branches.

#5 - 10/16/2018 11:23 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.3: REQUIRED, 2.4: REQUIRED, 2.5: REQUIRED to 2.3: REQUIRED, 2.4: REQUIRED, 2.5: DONE

ruby_2_5 r65100 merged revision(s) 64913.

#6 - 10/17/2018 08:11 AM - usa (Usaku NAKAMURA)

- Backport changed from 2.3: REQUIRED, 2.4: REQUIRED, 2.5: DONE to 2.3: REQUIRED, 2.4: DONE, 2.5: DONE

ruby_2_4 r65110 merged revision(s) 64913.

#7 - 10/17/2018 09:46 AM - usa (Usaku NAKAMURA)

- Backport changed from 2.3: REQUIRED, 2.4: DONE, 2.5: DONE to 2.3: DONE, 2.4: DONE, 2.5: DONE

ruby_2_3 r65119 merged revision(s) 64913.