Backport193 - Backport #8431

File.read() crash on Win32SP3 32bit

05/21/2013 10:47 PM - galnaktar (Oleg K)

Status:	Closed	
Priority:	Normal	
Assignee:	usa (Usaku NAKAMURA)	

Description

Open existing empty file, seek on 0xFFFFFFFF(4294967295) and trying to read 1 byte.

c:\Ruby200\bin>irb
DL is deprecated, please use Fiddle
irb(main):001:0> f = File.open("1", "w")
=> #File:1
irb(main):002:0> f.close
=> nil
irb(main):003:0> f = File.open("1", "rb")
=> #File:1
irb(main):004:0> f.seek(4294967295)
=> 0
irb(main):005:0> f.read(1)
(irb):5: [BUG] rb_sys_fail_str(1) - errno == 0
ruby 2.0.0p195 (2013-05-14) [i386-mingw32]

-- Control frame information ---
c:0019 p:---- s:0076 e:000075 CFUNC :read
c:0018 p:0007 s:0072 e:000071 EVAL (irb):5 [FINISH]
c:0017 p:---- s:0070 e:000069 CFUNC :eval
c:0016 p:0024 s:0063 e:000062 METHOD c:/Ruby200/lib/ruby/2.0.0/irb/workspace.rb:

Associated revisions

Revision a815b56d - 05/22/2013 06:19 AM - nobu (Nobuyoshi Nakada)

win32.c: check error of SetFilePointer

- win32/win32.c (setup_overlapped): check the error code in addition to the result of SetFilePointer() to determine if an error occurred, because INVALID_SET_FILE_POINTER is a valid value. [ruby-core:55098] [Bug #8431]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@40888 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 40888 - 05/22/2013 06:19 AM - nobu (Nobuyoshi Nakada)

win32.c: check error of SetFilePointer

- win32/win32.c (setup_overlapped): check the error code in addition to the result of SetFilePointer() to determine if an error occurred, because INVALID_SET_FILE_POINTER is a valid value. [ruby-core:55098] [Bug #8431]

Revision 40888 - 05/22/2013 06:19 AM - nobu (Nobuyoshi Nakada)

win32.c: check error of SetFilePointer

- win32/win32.c (setup_overlapped): check the error code in addition to the result of SetFilePointer() to determine if an error occurred, because INVALID_SET_FILE_POINTER is a valid value. [ruby-core:55098] [Bug #8431]

Revision 40888 - 05/22/2013 06:19 AM - nobu (Nobuyoshi Nakada)

win32.c: check error of SetFilePointer

- win32/win32.c (setup_overlapped): check the error code in addition to the result of SetFilePointer() to determine if an error occurred, because INVALID_SET_FILE_POINTER is a valid value. [ruby-core:55098] [Bug #8431]

Revision 40888 - 05/22/2013 06:19 AM - nobu (Nobuyoshi Nakada)

win32.c: check error of SetFilePointer

- win32/win32.c (setup_overlapped): check the error code in addition to the result of SetFilePointer() to determine if an error occurred, because INVALID_SET_FILE_POINTER is a valid value. [ruby-core:55098] [Bug #8431]

Revision 40888 - 05/22/2013 06:19 AM - nobu (Nobuyoshi Nakada)

win32.c: check error of SetFilePointer

- win32/win32.c (setup_overlapped): check the error code in addition to the result of SetFilePointer() to determine if an error occurred, because INVALID_SET_FILE_POINTER is a valid value. [ruby-core:55098] [Bug #8431]

Revision 40888 - 05/22/2013 06:19 AM - nobu (Nobuyoshi Nakada)

win32.c: check error of SetFilePointer

- win32/win32.c (setup_overlapped): check the error code in addition to the result of SetFilePointer() to determine if an error occurred, because INVALID_SET_FILE_POINTER is a valid value. [ruby-core:55098] [Bug #8431]

Revision ded54cb8 - 05/23/2013 02:14 AM - nobu (Nobuyoshi Nakada)

test_io.rb: test for write

- test/ruby/test_io.rb (TestIO#test_write_32bit_boundary): add test for write part. [ruby-core:55098] [Bug #8431]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@40894 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 40894 - 05/23/2013 02:14 AM - nobu (Nobuyoshi Nakada)

test_io.rb: test for write

- test/ruby/test_io.rb (TestIO#test_write_32bit_boundary): add test for write part. [ruby-core:55098] [Bug #8431]

Revision 40894 - 05/23/2013 02:14 AM - nobu (Nobuyoshi Nakada)

test_io.rb: test for write

- test/ruby/test_io.rb (TestIO#test_write_32bit_boundary): add test for write part. [ruby-core:55098] [Bug #8431]

Revision 40894 - 05/23/2013 02:14 AM - nobu (Nobuyoshi Nakada)

test_io.rb: test for write

- test/ruby/test_io.rb (TestIO#test_write_32bit_boundary): add test for write part. [ruby-core:55098] [Bug #8431]

Revision 40894 - 05/23/2013 02:14 AM - nobu (Nobuyoshi Nakada)

test_io.rb: test for write

- test/ruby/test_io.rb (TestIO#test_write_32bit_boundary): add test for write part. [ruby-core:55098] [Bug #8431]

Revision 40894 - 05/23/2013 02:14 AM - nobu (Nobuyoshi Nakada)

test_io.rb: test for write

- test/ruby/test_io.rb (TestIO#test_write_32bit_boundary): add test for write part. [ruby-core:55098] [Bug #8431]

Revision 40894 - 05/23/2013 02:14 AM - nobu (Nobuyoshi Nakada)

test_io.rb: test for write

- test/ruby/test_io.rb (TestIO#test_write_32bit_boundary): add test for write part. [ruby-core:55098] [Bug #8431]

Revision e377d3bb - 06/03/2013 03:49 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 40887,40888,40894,40896: [Backport #8431]

```
* win32/win32.c (setup_overlapped, finish_overlapped): extract from
  rb_w32_read() and rb_w32_write().

* win32/win32.c (setup_overlapped): check the error code in addition
  to the result of SetFilePointer() to determine if an error occurred,
  because INVALID_SET_FILE_POINTER is a valid value.
  [ruby-core:55098] [Bug #8431]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_0_0@41056 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 6ef15ce5 - 06/05/2013 03:38 AM - usa (Usaku NAKAMURA)

merge revision(s) 40887,40888,40894,40896: [Backport #8431]

```
    * win32/win32.c (setup_overlapped, finish_overlapped): extract from
      rb_w32_read() and rb_w32_write().

    * win32/win32.c (setup_overlapped): check the error code in addition
      to the result of SetFilePointer() to determine if an error occurred,
      because INVALID_SET_FILE_POINTER is a valid value.
      [ruby-core:55098] [Bug #8431]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_3@41082 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 41082 - 06/05/2013 03:38 AM - usa (Usaku NAKAMURA)

merge revision(s) 40887,40888,40894,40896: [Backport #8431]

```
* win32/win32.c (setup_overlapped, finish_overlapped): extract from
  rb_w32_read() and rb_w32_write().

* win32/win32.c (setup_overlapped): check the error code in addition
  to the result of SetFilePointer() to determine if an error occurred,
  because INVALID_SET_FILE_POINTER is a valid value.
  [ruby-core:55098] [Bug #8431]
```

History

#1 - 05/22/2013 09:54 AM - phasis68 (Heesob Park)

This bug is due to the invalid error checking of SetFilePointer function.
The constant INVALID_SET_FILE_POINTER is defined as (DWORD)-1 and is same to 0xFFFFFFFF(4294967295).

I can see the following sentences in the documentation of SetFilePointer function:
Because INVALID_SET_FILE_POINTER is a valid value for the low-order DWORD of the new file pointer, you must check both the return value of the function and the error code returned by GetLastError to determine whether or not an error has occurred. If an error has occurred, the return value of SetFilePointer is INVALID_SET_FILE_POINTER and GetLastError returns a value other than NO_ERROR.

Refer to http://msdn.microsoft.com/en-us/library/windows/desktop/aa365541(v=vs.85).aspx

Here is a patch:
diff --git a/win32.c b/win32.c.new
index 318af2f..79a49d4 100644
--- a/win32.c
+++ b/win32.c.new
@@ -6084,8 +6084,8 @@ rb_w32_read(int fd, void *buf, size_t size)
#ifndef INVALID_SET_FILE_POINTER
#define INVALID_SET_FILE_POINTER ((DWORD)-1)
#endif

- if (low == INVALID_SET_FILE_POINTER) {
- errno = map_errno(GetLastError());
- if (low == INVALID_SET_FILE_POINTER && (err = GetLastError()) != NO_ERROR) {
- errno = map_errno(err); MTHREAD_ONLY(LeaveCriticalSection(&_pioinfo(fd)->lock)); return -1; } @@ -6228,8 +6228,8 @@ rb_w32_write(int fd, const void *buf, size_t size) #ifndef INVALID_SET_FILE_POINTER #define INVALID_SET_FILE_POINTER ((DWORD)-1) #endif
- if (low == INVALID_SET_FILE_POINTER) {
- errno = map_errno(GetLastError());
- if (low == INVALID_SET_FILE_POINTER && (err = GetLastError()) != NO_ERROR) {
- errno = map_errno(err); MTHREAD_ONLY(LeaveCriticalSection(&_pioinfo(fd)->lock)); return -1; }

#2 - 05/22/2013 03:19 PM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r40888.
Oleg, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

---

win32.c: check error of SetFilePointer

- win32/win32.c (setup_overlapped): check the error code in addition to the result of SetFilePointer() to determine if an error occurred, because INVALID_SET_FILE_POINTER is a valid value. [ruby-core:55098] [Bug #8431]

#3 - 05/22/2013 03:21 PM - nobu (Nobuyoshi Nakada)

- Backport changed from 1.9.3: UNKNOWN, 2.0.0: UNKNOWN to 1.9.3: REQUIRED, 2.0.0: REQUIRED

#4 - 05/22/2013 03:21 PM - nobu (Nobuyoshi Nakada)

- Assignee changed from cruby-windows to nagachika (Tomoyuki Chikanaga)

- Tracker changed from Bug to Backport

- Project changed from Ruby trunk to Backport200

- Category deleted (platform/windows)

- Status changed from Closed to Assigned

#5 - 05/22/2013 04:47 PM - phasis68 (Heesob Park)

The change set r40888 is not complete.
As I pointed out the above patch, there are two SetFilePointer checking.
The invalid SetFilePointer check is still remains in the rb_w32_write function.

Here is write part segfault.

```
C:\Users\phasis>irb
DL is deprecated, please use Fiddle
irb(main):001:0> f = File.open('a','wb')
=> #File:a
irb(main):002:0> f.seek(0xffffffff)
=> 0
irb(main):003:0> f.write('1')
=> 1
irb(main):004:0> f.tell
(irb):4: [BUG] rb_sys_fail() - errno == 0
ruby 2.0.0p195 (2013-05-14) [i386-mingw32]

-- Control frame information -----------------------------------------------
c:0019 p:---- s:0075 e:000074 CFUNC  :tell
c:0018 p:0006 s:0072 e:000071 EVAL   (irb):4 [FINISH]
c:0017 p:---- s:0070 e:000069 CFUNC  :eval
c:0016 p:0024 s:0063 e:000062 METHOD C:/Ruby200/lib/ruby/2.0.0/irb/workspace.rb:
86
c:0015 p:0025 s:0056 e:000054 METHOD C:/Ruby200/lib/ruby/2.0.0/irb/context.rb:38
0
c:0014 p:0022 s:0050 e:000049 BLOCK  C:/Ruby200/lib/ruby/2.0.0/irb.rb:492
c:0013 p:0040 s:0042 e:000041 METHOD C:/Ruby200/lib/ruby/2.0.0/irb.rb:624
c:0012 p:0009 s:0037 e:000036 BLOCK  C:/Ruby200/lib/ruby/2.0.0/irb.rb:489
c:0011 p:0118 s:0033 e:000032 BLOCK  C:/Ruby200/lib/ruby/2.0.0/irb/ruby-lex.rb:2
47 [FINISH]
c:0010 p:---- s:0030 e:000029 CFUNC  :loop
c:0009 p:0007 s:0027 e:000026 BLOCK  C:/Ruby200/lib/ruby/2.0.0/irb/ruby-lex.rb:2
33 [FINISH]
c:0008 p:---- s:0025 e:000024 CFUNC  :catch
c:0007 p:0015 s:0021 e:000020 METHOD C:/Ruby200/lib/ruby/2.0.0/irb/ruby-lex.rb:2
32
c:0006 p:0030 s:0018 E:000564 METHOD C:/Ruby200/lib/ruby/2.0.0/irb.rb:488
c:0005 p:0008 s:0015 e:000014 BLOCK  C:/Ruby200/lib/ruby/2.0.0/irb.rb:397 [FINIS
H]
c:0004 p:---- s:0013 e:000012 CFUNC  :catch
c:0003 p:0143 s:0009 E:0000d4 METHOD C:/Ruby200/lib/ruby/2.0.0/irb.rb:396
c:0002 p:0031 s:0004 E:001d0c EVAL   C:/Ruby200/bin/irb:12 [FINISH]
c:0001 p:0000 s:0002 E:0023dc TOP    [FINISH]

C:/Ruby200/bin/irb:12:in <main>'
C:/Ruby200/lib/ruby/2.0.0/irb.rb:396:instart'
C:/Ruby200/lib/ruby/2.0.0/irb.rb:396:in catch'
C:/Ruby200/lib/ruby/2.0.0/irb.rb:397:inblock in start'
C:/Ruby200/lib/ruby/2.0.0/irb.rb:488:in eval_input'
C:/Ruby200/lib/ruby/2.0.0/irb/ruby-lex.rb:232:ineach_top_level_statement'
C:/Ruby200/lib/ruby/2.0.0/irb/ruby-lex.rb:232:in catch'
C:/Ruby200/lib/ruby/2.0.0/irb/ruby-lex.rb:233:inblock in each_top_level_statem
ent'
C:/Ruby200/lib/ruby/2.0.0/irb/ruby-lex.rb:233:in loop'
C:/Ruby200/lib/ruby/2.0.0/irb/ruby-lex.rb:247:inblock (2 levels) in each_top_l
evel_statement'
C:/Ruby200/lib/ruby/2.0.0/irb.rb:489:in block in eval_input'
C:/Ruby200/lib/ruby/2.0.0/irb.rb:624:insignal_status'
C:/Ruby200/lib/ruby/2.0.0/irb.rb:492:in block (2 levels) in eval_input'
C:/Ruby200/lib/ruby/2.0.0/irb/context.rb:380:inevaluate'
```

C:/Ruby200/lib/ruby/2.0.0/irb/workspace.rb:86:in evaluate'
C:/Ruby200/lib/ruby/2.0.0/irb/workspace.rb:86:ineval'
(irb):4:in irb_binding'
(irb):4:intell'

#6 - 05/22/2013 10:11 PM - luislavena (Luis Lavena)

- Assignee changed from nagachika (Tomoyuki Chikanaga) to nobu (Nobuyoshi Nakada)

- % Done changed from 100 to 50

nobu-san, do you want me to commit the missing fix?

#7 - 05/23/2013 11:15 AM - nobu (Nobuyoshi Nakada)

- Tracker changed from Backport to Bug

- Project changed from Backport200 to Ruby trunk

- Status changed from Assigned to Open

#8 - 05/23/2013 11:17 AM - nobu (Nobuyoshi Nakada)

- Category set to platform/windows

- ruby -v set to 2.1.0

Oops, [Backport] ticket can't catch the commit on trunk?
I added the test for write at r80894 now.

#9 - 05/23/2013 11:18 AM - nobu (Nobuyoshi Nakada)

- % Done changed from 50 to 100

#10 - 05/23/2013 11:18 AM - nobu (Nobuyoshi Nakada)

- Backport set to 1.9.3: REQUIRED, 2.0.0: REQUIRED

#11 - 05/23/2013 11:19 AM - nobu (Nobuyoshi Nakada)

- Tracker changed from Bug to Backport

- Project changed from Ruby trunk to Backport200

- Category deleted (platform/windows)

- Status changed from Open to Assigned

- Assignee changed from nobu (Nobuyoshi Nakada) to nagachika (Tomoyuki Chikanaga)

#12 - 05/23/2013 11:21 AM - nobu (Nobuyoshi Nakada)

Calls to SetFilePointer() are extracted as a new function at r40887, and r40888 fixed it.

#13 - 05/23/2013 11:57 AM - nobu (Nobuyoshi Nakada)

- Tracker changed from Backport to Bug

- Project changed from Backport200 to Ruby trunk

#14 - 05/23/2013 12:03 PM - nobu (Nobuyoshi Nakada)

- Category set to platform/windows

- Backport set to 1.9.3: REQUIRED, 2.0.0: REQUIRED

- ruby -v set to 2.1.0

r40896 is needed too.

#15 - 05/23/2013 12:03 PM - nobu (Nobuyoshi Nakada)

- Tracker changed from Bug to Backport

- Project changed from Ruby trunk to Backport200

- Category deleted (platform/windows)

#16 - 06/04/2013 12:49 AM - nagachika (Tomoyuki Chikanaga)

- Status changed from Assigned to Closed

This issue was solved with changeset r41056.
Oleg, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

---

merge revision(s) 40887,40888,40894,40896: [Backport #8431]

```
* win32/win32.c (setup_overlapped, finish_overlapped): extract from
  rb_w32_read() and rb_w32_write().

* win32/win32.c (setup_overlapped): check the error code in addition
  to the result of SetFilePointer() to determine if an error occurred,
  because INVALID_SET_FILE_POINTER is a valid value.
  [ruby-core:55098] [Bug #8431]
```

#17 - 06/04/2013 12:50 AM - nagachika (Tomoyuki Chikanaga)

- Project changed from Backport200 to Backport193

- Status changed from Closed to Assigned

- Assignee changed from nagachika (Tomoyuki Chikanaga) to usa (Usaku NAKAMURA)

backport for 1.9.3 is also required?

#18 - 06/05/2013 12:38 PM - usa (Usaku NAKAMURA)

- Status changed from Assigned to Closed

This issue was solved with changeset r41082.
Oleg, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

---

merge revision(s) 40887,40888,40894,40896: [Backport #8431]

```
* win32/win32.c (setup_overlapped, finish_overlapped): extract from
  rb_w32_read() and rb_w32_write().

* win32/win32.c (setup_overlapped): check the error code in addition
  to the result of SetFilePointer() to determine if an error occurred,
  because INVALID_SET_FILE_POINTER is a valid value.
  [ruby-core:55098] [Bug #8431]
```