Ruby master - Bug #11854

Socket.for_fd(-1) causes segmentaion fault on mingw32.

12/21/2015 09:43 AM - phasis68 (Heesob Park)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.3.0dev (2015-12-20 trunk 53220) [i386-mingw32]	**Backport:**	2.0.0: REQUIRED, 2.1: DONE, 2.2: DONE

Description

The following command causes segmentation fault on mingw32 built version

```
C:>ruby -rsocket -ve 'Socket.for_fd(-1)'

-e:1: [BUG] rb_update_max_fd: invalid fd (-1) given.
ruby 2.3.0dev (2015-12-20 trunk 53220) [i386-mingw32]

-- Control frame information -----------------------------------------------
c:0003 p:---- s:0008 e:000007 CFUNC  :for_fd
c:0002 p:0014 s:0004 E:001a68 EVAL   -e:1 [FINISH]
c:0001 p:0000 s:0002 E:0008e0 (none) [FINISH]

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

-- C level backtrace information -------------------------------------------
C:\WINDOWS\SYSTEM32\ntdll.dll(ZwWaitForSingleObject+0xc) [0x771B6B1C]
C:\WINDOWS\SYSTEM32\KERNELBASE.dll(WaitForSingleObject+0x12) [0x76E4DFF2]
c:\usr\local\bin\msvcrt-ruby230.dll(rb_vm_bugreport+0xaa) [0x6305F47A]
c:\usr\local\bin\msvcrt-ruby230.dll(rb_bug+0x4a) [0x62F05F5A]
c:\usr\local\bin\msvcrt-ruby230.dll(rb_update_max_fd+0x65) [0x62F3EE65] [0x6E60169D] [0x6E60A829]
c:\usr\local\bin\msvcrt-ruby230.dll(rb_error_arity+0x20a) [0x6304949A]
c:\usr\local\bin\msvcrt-ruby230.dll(rb_vm_invoke_proc+0x33d) [0x6305485D]
c:\usr\local\bin\msvcrt-ruby230.dll(rb_vm_invoke_proc+0x782) [0x63054CA2]
c:\usr\local\bin\msvcrt-ruby230.dll(rb_vm_localjump_error+0xf7f) [0x6304EEDF]
c:\usr\local\bin\msvcrt-ruby230.dll(rb_vm_localjump_error+0x5b97) [0x63053AF7]
c:\usr\local\bin\msvcrt-ruby230.dll(rb_check_copyable+0x3202) [0x62F0B402]
c:\usr\local\bin\msvcrt-ruby230.dll(ruby_run_node+0x2d) [0x62F0E6AD] [0x0040287F] [0x004013FA]
C:\WINDOWS\SYSTEM32\KERNEL32.DLL(BaseThreadInitThunk+0x24) [0x76C338F4]
C:\WINDOWS\SYSTEM32\ntdll.dll(RtlUnicodeStringToInteger+0x253) [0x771A56C3]

-- Other runtime information -----------------------------------------------

* Loaded script: -e

* Loaded features:

    0 enumerator.so
    1 thread.rb
    2 rational.so
    3 complex.so
    4 c:/usr/local/lib/ruby/2.3.0/i386-mingw32/enc/encdb.so
    5 c:/usr/local/lib/ruby/2.3.0/i386-mingw32/enc/trans/transdb.so
    6 c:/usr/local/lib/ruby/2.3.0/i386-mingw32/enc/cp949.so
    7 c:/usr/local/lib/ruby/2.3.0/unicode_normalize.rb
    8 c:/usr/local/lib/ruby/2.3.0/i386-mingw32/rbconfig.rb
    9 c:/usr/local/lib/ruby/2.3.0/rubygems/compatibility.rb
   10 c:/usr/local/lib/ruby/2.3.0/rubygems/defaults.rb
   11 c:/usr/local/lib/ruby/2.3.0/rubygems/deprecate.rb
   12 c:/usr/local/lib/ruby/2.3.0/rubygems/errors.rb
```

```
   13 c:/usr/local/lib/ruby/2.3.0/rubygems/version.rb
   14 c:/usr/local/lib/ruby/2.3.0/rubygems/requirement.rb
   15 c:/usr/local/lib/ruby/2.3.0/rubygems/platform.rb
   16 c:/usr/local/lib/ruby/2.3.0/rubygems/basic_specification.rb
   17 c:/usr/local/lib/ruby/2.3.0/rubygems/stub_specification.rb
   18 c:/usr/local/lib/ruby/2.3.0/rubygems/util/list.rb
   19 c:/usr/local/lib/ruby/2.3.0/i386-mingw32/stringio.so
   20 c:/usr/local/lib/ruby/2.3.0/rubygems/specification.rb
   21 c:/usr/local/lib/ruby/2.3.0/rubygems/exceptions.rb
   22 c:/usr/local/lib/ruby/2.3.0/rubygems/core_ext/kernel_gem.rb
   23 c:/usr/local/lib/ruby/2.3.0/monitor.rb
   24 c:/usr/local/lib/ruby/2.3.0/rubygems/core_ext/kernel_require.rb
   25 c:/usr/local/lib/ruby/2.3.0/rubygems.rb
   26 c:/usr/local/lib/ruby/2.3.0/rubygems/path_support.rb
   27 c:/usr/local/lib/ruby/2.3.0/rubygems/dependency.rb
   28 c:/usr/local/lib/ruby/gems/2.3.0/gems/did_you_mean-1.0.0.rc1/lib/did_you_mean/version.rb
   29 c:/usr/local/lib/ruby/gems/2.3.0/gems/did_you_mean-1.0.0.rc1/lib/did_you_mean/core_ext/name_
error.rb
   30 c:/usr/local/lib/ruby/gems/2.3.0/gems/did_you_mean-1.0.0.rc1/lib/did_you_mean/levenshtein.rb
   31 c:/usr/local/lib/ruby/gems/2.3.0/gems/did_you_mean-1.0.0.rc1/lib/did_you_mean/jaro_winkler.r
b
   32 c:/usr/local/lib/ruby/gems/2.3.0/gems/did_you_mean-1.0.0.rc1/lib/did_you_mean/spell_checkabl
e.rb
   33 c:/usr/local/lib/ruby/2.3.0/delegate.rb
   34 c:/usr/local/lib/ruby/gems/2.3.0/gems/did_you_mean-1.0.0.rc1/lib/did_you_mean/spell_checkers
/name_error_checkers/class_name_checker.rb
   35 c:/usr/local/lib/ruby/gems/2.3.0/gems/did_you_mean-1.0.0.rc1/lib/did_you_mean/spell_checkers
/name_error_checkers/variable_name_checker.rb
   36 c:/usr/local/lib/ruby/gems/2.3.0/gems/did_you_mean-1.0.0.rc1/lib/did_you_mean/spell_checkers
/name_error_checkers.rb
   37 c:/usr/local/lib/ruby/gems/2.3.0/gems/did_you_mean-1.0.0.rc1/lib/did_you_mean/spell_checkers
/method_name_checker.rb
   38 c:/usr/local/lib/ruby/gems/2.3.0/gems/did_you_mean-1.0.0.rc1/lib/did_you_mean/spell_checkers
/null_checker.rb
   39 c:/usr/local/lib/ruby/gems/2.3.0/gems/did_you_mean-1.0.0.rc1/lib/did_you_mean/formatter.rb
   40 c:/usr/local/lib/ruby/gems/2.3.0/gems/did_you_mean-1.0.0.rc1/lib/did_you_mean.rb
   41 c:/usr/local/lib/ruby/2.3.0/i386-mingw32/socket.so
   42 c:/usr/local/lib/ruby/2.3.0/i386-mingw32/io/wait.so
   43 c:/usr/local/lib/ruby/2.3.0/socket.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.
```

Here is a patch for this issue:

```
--- init.c  Tue Nov 24 07:57:29 2015
+++ init.c.new  Mon Dec 21 18:31:28 2015
@@ -61,9 +61,9 @@
 {
     rb_io_t *fp;

-    rb_update_max_fd(fd);
     if (!is_socket(fd))
         rb_raise(rb_eArgError, "not a socket file descriptor");
+    rb_update_max_fd(fd);

     MakeOpenFile(sock, fp);
     fp->fd = fd;
```

Associated revisions

Revision 409e53de - 12/21/2015 06:57 PM - normal

avoid rb_bug on BasicSocket.for_fd(-1)

- ext/socket/init.c (rsock_init_sock): check FD after validating
- test/socket/test_basicsocket.rb (test_for_fd): new [ruby-core:72418] [Bug #11854]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@53231 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 53231 - 12/21/2015 06:57 PM - normalperson (Eric Wong)

avoid rb_bug on BasicSocket.for_fd(-1)

- ext/socket/init.c (rsock_init_sock): check FD after validating
- test/socket/test_basicsocket.rb (test_for_fd): new [ruby-core:72418] [Bug #11854]

Revision 53231 - 12/21/2015 06:57 PM - normal

avoid rb_bug on BasicSocket.for_fd(-1)

- ext/socket/init.c (rsock_init_sock): check FD after validating
- test/socket/test_basicsocket.rb (test_for_fd): new [ruby-core:72418] [Bug #11854]

Revision 53231 - 12/21/2015 06:57 PM - normal

avoid rb_bug on BasicSocket.for_fd(-1)

- ext/socket/init.c (rsock_init_sock): check FD after validating
- test/socket/test_basicsocket.rb (test_for_fd): new [ruby-core:72418] [Bug #11854]

Revision 53231 - 12/21/2015 06:57 PM - normal

avoid rb_bug on BasicSocket.for_fd(-1)

- ext/socket/init.c (rsock_init_sock): check FD after validating
- test/socket/test_basicsocket.rb (test_for_fd): new [ruby-core:72418] [Bug #11854]

Revision 53231 - 12/21/2015 06:57 PM - normal

avoid rb_bug on BasicSocket.for_fd(-1)

- ext/socket/init.c (rsock_init_sock): check FD after validating
- test/socket/test_basicsocket.rb (test_for_fd): new [ruby-core:72418] [Bug #11854]

Revision c9eefd56 - 02/25/2016 08:45 AM - usa (Usaku NAKAMURA)

merge revision(s) 53231,53244: [Backport #11854]

```
    * ext/socket/init.c (rsock_init_sock): check FD after validating

    * test/socket/test_basicsocket.rb (test_for_fd): new
      [ruby-core:72418] [Bug #11854]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@53923 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 53923 - 02/25/2016 08:45 AM - usa (Usaku NAKAMURA)

merge revision(s) 53231,53244: [Backport #11854]

```
* ext/socket/init.c (rsock_init_sock): check FD after validating

* test/socket/test_basicsocket.rb (test_for_fd): new
  [ruby-core:72418] [Bug #11854]
```

Revision f429ee01 - 03/08/2016 06:49 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 52605,53231,53244: [Backport #11854]

```
    init.c: is_socket

    * ext/socket/init.c (is_socket): extract predicate to see if the
```

given fd is a socket.
* ext/socket/init.c (rsock_init_sock): check FD after validating

```
    * test/socket/test_basicsocket.rb (test_for_fd): new
```

```
    [ruby-core:72418] [Bug #11854]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@54038 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 54038 - 03/08/2016 06:49 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 52605,53231,53244: [Backport #11854]

```
init.c: is_socket

* ext/socket/init.c (is_socket): extract predicate to see if the
```

given fd is a socket.
* ext/socket/init.c (rsock_init_sock): check FD after validating

```
* test/socket/test_basicsocket.rb (test_for_fd): new
  [ruby-core:72418] [Bug #11854]
```

History

#1 - 12/21/2015 10:18 AM - normalperson (Eric Wong)

Proposed fix (not sure about the error message saying "fstat(2)", now...)

Subject: [PATCH] avoid rb_bug on BasicSocket.for_fd(-1)

- ext/socket/init.c (rsock_init_sock): check FD after validating
- test/socket/test_basicsocket.rb (test_for_fd): new [ruby-core:72418] [Bug #11854] --- ext/socket/init.c | 2 +- test/socket/test_basicsocket.rb | 11 ++++++++++ 2 files changed, 12 insertions(+), 1 deletion(-)

diff --git a/ext/socket/init.c b/ext/socket/init.c
index d071102..bd06926 100644
--- a/ext/socket/init.c
+++ b/ext/socket/init.c
@@ -61,10 +61,10 @@ rsock_init_sock(VALUE sock, int fd)
{
rb_io_t *fp;

- rb_update_max_fd(fd);
  if (!is_socket(fd))
  rb_raise(rb_eArgError, "not a socket file descriptor");

- rb_update_max_fd(fd);
  MakeOpenFile(sock, fp);
  fp->fd = fd;
  fp->mode = FMODE_READWRITE|FMODE_DUPLEX;
  diff --git a/test/socket/test_basicsocket.rb b/test/socket/test_basicsocket.rb
  index 227034e..52732f1 100644
  --- a/test/socket/test_basicsocket.rb
  +++ b/test/socket/test_basicsocket.rb
  @@ -133,4 +133,15 @@ def test_close_write
  end
  end

- def test_for_fd
- assert_raise(Errno::EBADF, '[ruby-core:72418] [Bug #11854]') do
- [redacted]
- end
- inet_stream do |sock|
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- end
- end

end if defined?(BasicSocket)

EW

#2 - 12/21/2015 06:57 PM - normalperson (Eric Wong)

- Backport changed from 2.0.0: UNKNOWN, 2.1: UNKNOWN, 2.2: UNKNOWN to 2.0.0: REQUIRED, 2.1: REQUIRED, 2.2: REQUIRED

Will commit patch as-is since 2.3 release is soon.

#3 - 12/21/2015 06:58 PM - Anonymous

- Status changed from Open to Closed

Applied in changeset r53231.

---

avoid rb_bug on BasicSocket.for_fd(-1)

- ext/socket/init.c (rsock_init_sock): check FD after validating
- test/socket/test_basicsocket.rb (test_for_fd): new [ruby-core:72418] [Bug #11854]

#4 - 02/25/2016 08:44 AM - usa (Usaku NAKAMURA)

- Backport changed from 2.0.0: REQUIRED, 2.1: REQUIRED, 2.2: REQUIRED to 2.0.0: REQUIRED, 2.1: DONE, 2.2: REQUIRED

ruby_2_1 r53923 merged revision(s) 53231,53244.

#5 - 03/08/2016 06:50 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.0.0: REQUIRED, 2.1: DONE, 2.2: REQUIRED to 2.0.0: REQUIRED, 2.1: DONE, 2.2: DONE

r52605, r53231 and r53244 were backported into ruby_2_2 branch at r54038.