Ruby master - Bug #6099
[BUG] probable buffer overflow
02/28/2012 01:53 PM - usa (Usaku NAKAMURA)

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>nobu (Nobuyoshi Nakada)</td>
</tr>
<tr>
<td>Target version:</td>
<td>2.0.0</td>
</tr>
</tbody>
</table>

ruby -v:
ruby 2.0.0dev (2012-02-27 trunk 34828) [i386-netbsdelf]

Backport:

Description
ふと思い立って以下のようなコードを実行してみたところ、表題の[BUG]となりました。
あんまり重大ではないと考えますが、一応報告しておきます。
他のメソッドでも似たようなことができるものと思います。
なお、プラットフォーム依存はないはずです。

% ruby -e 'r, w = IO.pipe
buf = " " * 100
Thread.new{p r.sysread(100, buf)}
Thread.pass
buf.replace("")
p buf.bytesize; w.write("a" * 100)
Thread.pass
'

Associated revisions
Revision 9b02a72d - 02/28/2012 09:33 AM - nobu (Nobuyoshi Nakada)
  • io.c (io_fread, io_getpartial, rb_io_sysread): set buffer size after check if readable, which can cause thread switch. [ruby-dev:45297][Bug #6099]
  git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@34846 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 34846 - 02/28/2012 09:33 AM - nobu (Nobuyoshi Nakada)
  • io.c (io_fread, io_getpartial, rb_io_sysread): set buffer size after check if readable, which can cause thread switch. [ruby-dev:45297][Bug #6099]

Revision 34846 - 02/28/2012 09:33 AM - nobu (Nobuyoshi Nakada)
  • io.c (io_fread, io_getpartial, rb_io_sysread): set buffer size after check if readable, which can cause thread switch. [ruby-dev:45297][Bug #6099]

Revision 34846 - 02/28/2012 09:33 AM - nobu (Nobuyoshi Nakada)
  • io.c (io_fread, io_getpartial, rb_io_sysread): set buffer size after check if readable, which can cause thread switch. [ruby-dev:45297][Bug #6099]

Revision 34846 - 02/28/2012 09:33 AM - nobu (Nobuyoshi Nakada)
  • io.c (io_fread, io_getpartial, rb_io_sysread): set buffer size after check if readable, which can cause thread switch. [ruby-dev:45297][Bug #6099]

Revision 34846 - 02/28/2012 09:33 AM - nobu (Nobuyoshi Nakada)
  • io.c (io_fread, io_getpartial, rb_io_sysread): set buffer size after check if readable, which can cause thread switch. [ruby-dev:45297][Bug #6099]

Revision 34846 - 02/28/2012 09:33 AM - nobu (Nobuyoshi Nakada)
  • io.c (io_fread, io_getpartial, rb_io_sysread): set buffer size after check if readable, which can cause thread switch. [ruby-dev:45297][Bug #6099]

Revision 34846 - 02/28/2012 09:33 AM - nobu (Nobuyoshi Nakada)
  • io.c (io_fread, io_getpartial, rb_io_sysread): set buffer size after check if readable, which can cause thread switch. [ruby-dev:45297][Bug #6099]

Revision 34846 - 02/28/2012 09:33 AM - nobu (Nobuyoshi Nakada)
  • io.c (io_fread, io_getpartial, rb_io_sysread): set buffer size after check if readable, which can cause thread switch. [ruby-dev:45297][Bug #6099]

Revision 34846 - 02/28/2012 09:33 AM - nobu (Nobuyoshi Nakada)
  • io.c (io_fread, io_getpartial, rb_io_sysread): set buffer size after check if readable, which can cause thread switch. [ruby-dev:45297][Bug #6099]

Revision 34846 - 02/28/2012 09:33 AM - nobu (Nobuyoshi Nakada)
  • io.c (io_fread, io_getpartial, rb_io_sysread): set buffer size after check if readable, which can cause thread switch. [ruby-dev:45297][Bug #6099]

Revision 34846 - 02/28/2012 09:33 AM - nobu (Nobuyoshi Nakada)
  • io.c (io_fread, io_getpartial, rb_io_sysread): set buffer size after check if readable, which can cause thread switch. [ruby-dev:45297][Bug #6099]

Revision 34846 - 02/28/2012 09:33 AM - nobu (Nobuyoshi Nakada)
  • io.c (io_fread, io_getpartial, rb_io_sysread): set buffer size after check if readable, which can cause thread switch. [ruby-dev:45297][Bug #6099]

History
#1 - 02/28/2012 03:33 PM - Glass_saga (Masaki Matsushita)

```ruby
require "fcntl"

r, w = IO.pipe
r.fcntl(Fcntl::F_SETFL, Fcntl::O_NONBLOCK)
buff = " " * 100
t = Thread.new { p r.readpartial(100, buff) }
sleep 0.1
Thread.pass
buff.replace("")
p buff.bytesize; w.write("a" * 100)
Thread.pass
t.join
```

#2 - 02/28/2012 06:33 PM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed
- % Done changed from 0 to 100

This issue was solved with changeset r34846.
Usaku, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- io.c (io_read, io_getpartial, rb_io_sysread): set buffer size after check if readable, which can cause thread switch. [ruby-dev:45297][Bug #6099]

#3 - 03/07/2012 10:49 AM - naruse (Yui NARUSE)

- Status changed from Closed to Assigned
- Assignee set to nobu (Nobuyoshi Nakada)
- Priority changed from 3 to Normal

Masaki Matsushita wrote:

```ruby
require "fcntl"

r, w = IO.pipe
r.fcntl(Fcntl::F_SETFL, Fcntl::O_NONBLOCK)
buff = " " * 100
t = Thread.new { p r.readpartial(100, buff) }
sleep 0.1
Thread.pass
buff.replace("")
p buff.bytesize; w.write("a" * 100)
Thread.pass
t.join
```

- IO#readpartial is nonblocking-flag insensitive.
- It blocks only if ios has no data immediately available.
- The later means that readpartial is nonblocking-flag insensitive.
- It blocks on the situation IO#sysread causes Errno::EWOULDBLOCK as if the fd is blocking mode.

#4 - 03/20/2012 11:28 AM - Glass_saga (Masaki Matsushita)

Yui NARUSE wrote:

```ruby
IO#readpartial
```
- It blocks only if ios has no data immediately available.
- The later means that readpartial is nonblocking-flag insensitive.
- It blocks on the situation IO#sysread causes Errno::EWOULDBLOCK as if the fd is blocking mode. 于是当fcntl(Fcntl::F_SETFL, Fcntl::O_NONBLOCK) 时 block 也会发生BUG，所以这种情况虽然合理但不是可接受的。

IO#readpartial も場合によっては block することがあります。

#5 - 03/21/2012 05:57 PM - naruse (Yui NARUSE)

- Status changed from Assigned to Closed