Ruby master - Bug #8728

strio_substr can put invalid pointer into substring

08/04/2013 06:30 AM - headius (Charles Nutter)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:	2.6		
ruby -v:	2.1.0-dev	**Backport:**	1.9.3: UNKNOWN, 2.0.0: UNKNOWN

Description

There's a bug in strio_substr when reading a zero-length string from a StringIO when the position is past the end of the internal string.

```
static VALUE
strio_substr(struct StringIO *ptr, long pos, long len)
{
VALUE str = ptr->string;
rb_encoding *enc = rb_enc_get(str);
long rlen = RSTRING_LEN(str) - pos;

if (len > rlen) len = rlen;
if (len < 0) len = 0;
return rb_enc_str_new(RSTRING_PTR(str)+pos, len, enc);

}
```

Logic in strio_read passes ptr->pos directly to this function:

```
...
if (NIL_P(str)) {
str = strio_substr(ptr, ptr->pos, len);
if (binary) rb_enc_associate(str, rb_ascii8bit_encoding());
}
...
```

Logic above will check if ptr->pos is >= the string length, but *only* if the requested length is greater than zero:

```
...
case 1:
if (!NIL_P(argv[0])) {
len = NUM2LONG(argv[0]);
if (len < 0) {
rb_raise(rb_eArgError, "negative length %ld given", len);
}
if (len > 0 && ptr->pos >= RSTRING_LEN(ptr->string)) {
if (!NIL_P(str)) rb_str_resize(str, 0);
return Qnil;
}
binary = 1;
break;
}
...
```

So the following code, which seeks way beyond the end of the StringIO string, ends up calling strio_substr with the position as-is, resulting in a RubyString pointing off into invalid memory:

```
sio = StringIO.new("")
sio.seek(10000000000)
str = sio.read(0)
```

It doesn't manifest as a crash, as far as I can tell, because the resulting string is of length zero. There's shortcuts in the string logic to never dereference the string's pointer if the length is zero.

However...the pointer is completely invalid. It seems like bad form to reference invalid memory, even if you're pretty sure you won't dereference it.

A simple fix would be to have strio_substr use some other ptr offset when pos does not point at valid memory, but I'm not sure what offset that should be. A better fix would probably be to have it always return a new empty string when len == 0.

I have ported much of this logic into JRuby and today could not figure out how pos gets validated before creating this string. As it turns out, it does not...so I will be doing the empty string fix in JRuby.

Associated revisions

Revision 7974fe6a - 08/03/2013 09:53 PM - headius (Charles Nutter)

- ext/stringio/stringio.c (strio_substr): Trivial fix for invalid pointer when len = 0 and pos outside of string. Bug #8728.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@42366 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 42366 - 08/03/2013 09:53 PM - headius (Charles Nutter)

- ext/stringio/stringio.c (strio_substr): Trivial fix for invalid pointer when len = 0 and pos outside of string. Bug #8728.

Revision 42366 - 08/03/2013 09:53 PM - headius (Charles Nutter)

- ext/stringio/stringio.c (strio_substr): Trivial fix for invalid pointer when len = 0 and pos outside of string. Bug #8728.

Revision 42366 - 08/03/2013 09:53 PM - headius (Charles Nutter)

- ext/stringio/stringio.c (strio_substr): Trivial fix for invalid pointer when len = 0 and pos outside of string. Bug #8728.

Revision 42366 - 08/03/2013 09:53 PM - headius (Charles Nutter)

- ext/stringio/stringio.c (strio_substr): Trivial fix for invalid pointer when len = 0 and pos outside of string. Bug #8728.

Revision 42366 - 08/03/2013 09:53 PM - headius (Charles Nutter)

- ext/stringio/stringio.c (strio_substr): Trivial fix for invalid pointer when len = 0 and pos outside of string. Bug #8728.

Revision 42366 - 08/03/2013 09:53 PM - headius (Charles Nutter)

- ext/stringio/stringio.c (strio_substr): Trivial fix for invalid pointer when len = 0 and pos outside of string. Bug #8728.

History

#1 - 08/04/2013 06:43 AM - headius (Charles Nutter)

I will go ahead and fix this with an empty string.

#2 - 08/04/2013 06:53 AM - headius (Charles Nutter)

- Status changed from Open to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r42366.
Charles, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- ext/stringio/stringio.c (strio_substr): Trivial fix for invalid pointer when len = 0 and pos outside of string. Bug #8728.