

Ruby - Bug #13034

rb_enc_ascget() does not handle 'needmore' error from rb_enc_precise_mbclen()

12/14/2016 12:20 PM - rhenium (Kazuki Yamaguchi)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:		
Backport:		2.1: UNKNOWN, 2.2: DONE, 2.3: DONE
Description		
rb_enc_ascget() stores the return value from rb_enc_precise_mbclen() that may return a negative value on error to 'unsigned int', and thus it overlooks errors due to incomplete UTF-16/32 byte sequence.		
This bug is visible from Ruby; for example, the following code gets stuck in infinite loop:		
<pre>str = "\x00".force_encoding("UTF-16BE") Regexp.quote(str) # Ruby freezes</pre>		

Associated revisions

Revision 201972ac4cf81d12a7018308b9e88400c5e61a9d - 12/14/2016 12:32 PM - rhenium (Kazuki Yamaguchi)

encoding.c: handle needmore error from rb_enc_precise_mbclen()

rb_enc_ascget() erroneously reports success even if the given byte sequence is incomplete, for non-ASCII compatible encoding strings.

rb_enc_precise_mbclen() may return a negative value on error, and thus rb_enc_ascget() must not store the return value in 'unsigned int'; otherwise the subsequent MBCLen_CHARFOUND_P() check won't catch the error. [ruby-core:78646] [Bug #13034]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@57078 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 201972ac - 12/14/2016 12:32 PM - rhenium (Kazuki Yamaguchi)

encoding.c: handle needmore error from rb_enc_precise_mbclen()

rb_enc_ascget() erroneously reports success even if the given byte sequence is incomplete, for non-ASCII compatible encoding strings.

rb_enc_precise_mbclen() may return a negative value on error, and thus rb_enc_ascget() must not store the return value in 'unsigned int'; otherwise the subsequent MBCLen_CHARFOUND_P() check won't catch the error. [ruby-core:78646] [Bug #13034]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@57078 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 745565052a915f8815cd5d3cf299ab4cba20c57c - 12/27/2016 10:52 AM - U.Nakamura

merge revision(s) 57078: [Backport #13034]

```
encoding.c: handle needmore error from rb_enc_precise_mbclen()
```

```
rb_enc_ascget() erroneously reports success even if the given byte
sequence is incomplete, for non-ASCII compatible encoding strings.
```

```
rb_enc_precise_mbclen() may return a negative value on error, and thus
rb_enc_ascget() must not store the return value in 'unsigned int';
otherwise the subsequent MBCLen_CHARFOUND_P() check won't catch the
error. [ruby-core:78646] [Bug #13034]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@57217 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 74556505 - 12/27/2016 10:52 AM - U.Nakamura

merge revision(s) 57078: [Backport #13034]

```
encoding.c: handle needmore error from rb_enc_precise_mbclen()
```

```
rb_enc_ascget() erroneously reports success even if the given byte
sequence is incomplete, for non-ASCII compatible encoding strings.
```

```
rb_enc_precise_mbclen() may return a negative value on error, and thus
rb_enc_ascget() must not store the return value in 'unsigned int';
otherwise the subsequent MBCLen_CHARFOUND_P() check won't catch the
error. [ruby-core:78646] [Bug #13034]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@57217 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision f327b5e23ce39b3dbe9ada818232731d7c70e39b - 01/16/2017 07:31 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 57078: [Backport #13034]

```
encoding.c: handle needmore error from rb_enc_precise_mbclen()
```

```
rb_enc_ascget() erroneously reports success even if the given byte
sequence is incomplete, for non-ASCII compatible encoding strings.
```

```
rb_enc_precise_mbclen() may return a negative value on error, and thus
rb_enc_ascget() must not store the return value in 'unsigned int';
otherwise the subsequent MBCLen_CHARFOUND_P() check won't catch the
error. [ruby-core:78646] [Bug #13034]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@57348 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision f327b5e2 - 01/16/2017 07:31 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 57078: [Backport #13034]

```
encoding.c: handle needmore error from rb_enc_precise_mbclen()
```

```
rb_enc_ascget() erroneously reports success even if the given byte
sequence is incomplete, for non-ASCII compatible encoding strings.
```

```
rb_enc_precise_mbclen() may return a negative value on error, and thus
rb_enc_ascget() must not store the return value in 'unsigned int';
otherwise the subsequent MBCLen_CHARFOUND_P() check won't catch the
error. [ruby-core:78646] [Bug #13034]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@57348 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 12/14/2016 12:32 PM - Anonymous

- Status changed from Open to Closed

Applied in changeset r57078.

```
encoding.c: handle needmore error from rb_enc_precise_mbclen()
```

```
rb_enc_ascget() erroneously reports success even if the given byte
sequence is incomplete, for non-ASCII compatible encoding strings.
```

```
rb_enc_precise_mbclen() may return a negative value on error, and thus
rb_enc_ascget() must not store the return value in 'unsigned int';
otherwise the subsequent MBCLen_CHARFOUND_P() check won't catch the
error. [ruby-core:78646] [Bug #13034]
```

#2 - 12/27/2016 10:52 AM - usa (Usaku NAKAMURA)

- Backport changed from 2.1: UNKNOWN, 2.2: REQUIRED, 2.3: REQUIRED to 2.1: UNKNOWN, 2.2: DONE, 2.3: REQUIRED

ruby_2_2 r57217 merged revision(s) 57078.

#3 - 01/16/2017 07:31 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.1: UNKNOWN, 2.2: DONE, 2.3: REQUIRED to 2.1: UNKNOWN, 2.2: DONE, 2.3: DONE

ruby_2_3 r57348 merged revision(s) 57078.