Ruby trunk - Bug #7040

gem install □□□□ gem □□□□□□□□□□□

09/20/2012 10:29 AM - hsbt (Hiroshi SHIBATA)

Status:	Closed		
Priority:	Normal		
Assignee:	nagachika (Tomoyuki Chikanaga)		
Target version:	2.0.0		
ruby -v:	ruby 2.0.0dev (2012-09-20 trunk 36993) [x86_64-darwin12.2.0]	**Backport:**	

Description

trunk □□□□ gem(□□□ libv8□)□□□□□□□□□□□□□□□□□□□□□□□□□□□

```
% gem i libv8
ERROR:  While executing gem ... (Zlib::BufError)
buffer error
```

Twitter □□ nagachika □□□□ Zlib □ GVL □□?□□□

Associated revisions

Revision f21ac99e - 10/08/2012 04:40 PM - nagachika (Tomoyuki Chikanaga)

- ext/zlib/zlib.c (zstream_run_func): don't call inflate() when z->stream.avail_in == 0. it return Z_BUF_ERROR. but deflate() could be called with z->stream->avail_in == 0 because it has hidden buffer in z->stream->state (opaque structure). fix for gem install error. [ruby-dev:46149] [Bug #7040]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@37119 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 37119 - 10/08/2012 04:40 PM - nagachika (Tomoyuki Chikanaga)

- ext/zlib/zlib.c (zstream_run_func): don't call inflate() when z->stream.avail_in == 0. it return Z_BUF_ERROR. but deflate() could be called with z->stream->avail_in == 0 because it has hidden buffer in z->stream->state (opaque structure). fix for gem install error. [ruby-dev:46149] [Bug #7040]

Revision 37119 - 10/08/2012 04:40 PM - nagachika (Tomoyuki Chikanaga)

- ext/zlib/zlib.c (zstream_run_func): don't call inflate() when z->stream.avail_in == 0. it return Z_BUF_ERROR. but deflate() could be called with z->stream->avail_in == 0 because it has hidden buffer in z->stream->state (opaque structure). fix for gem install error. [ruby-dev:46149] [Bug #7040]

Revision 37119 - 10/08/2012 04:40 PM - nagachika (Tomoyuki Chikanaga)

- ext/zlib/zlib.c (zstream_run_func): don't call inflate() when z->stream.avail_in == 0. it return Z_BUF_ERROR. but deflate() could be called with z->stream->avail_in == 0 because it has hidden buffer in z->stream->state (opaque structure). fix for gem install error. [ruby-dev:46149] [Bug #7040]

Revision 37119 - 10/08/2012 04:40 PM - nagachika (Tomoyuki Chikanaga)

- ext/zlib/zlib.c (zstream_run_func): don't call inflate() when z->stream.avail_in == 0. it return Z_BUF_ERROR. but deflate() could be called with z->stream->avail_in == 0 because it has hidden buffer in z->stream->state (opaque structure). fix for gem install error. [ruby-dev:46149] [Bug #7040]

Revision 37119 - 10/08/2012 04:40 PM - nagachika (Tomoyuki Chikanaga)

- ext/zlib/zlib.c (zstream_run_func): don't call inflate() when z->stream.avail_in == 0. it return Z_BUF_ERROR. but deflate() could be called with z->stream->avail_in == 0 because it has hidden buffer in z->stream->state (opaque structure). fix for gem install error. [ruby-dev:46149] [Bug #7040]

Revision 37119 - 10/08/2012 04:40 PM - nagachika (Tomoyuki Chikanaga)

- ext/zlib/zlib.c (zstream_run_func): don't call inflate() when z->stream.avail_in == 0. it return Z_BUF_ERROR. but deflate() could be called with z->stream->avail_in == 0 because it has hidden buffer in z->stream->state (opaque structure). fix for gem install error. [ruby-dev:46149] [Bug #7040]

History

#1 - 09/20/2012 11:57 AM - nagachika (Tomoyuki Chikanaga)

- Assignee set to drbrain (Eric Hodel)

Hello,

I'd like to switch to ruby-core, but I don't know how to do it on redmine...

Anyway, I've found that zstream_run_func() leaks Z_BUF_ERROR because inflate() could return Z_BUF_ERROR even when z->stream.avail_out > 0.
My tiny patch below prevent the exception, but I'm not confident at all it's right way to fix this issue.

diff --git a/ext/zlib/zlib.c b/ext/zlib/zlib.c
index 6135e82..bcf289f 100644
--- a/ext/zlib/zlib.c
+++ b/ext/zlib/zlib.c
@@ -987,6 +987,7 @@ zstream_run_func(void *ptr)

```
    if (z->stream.avail_out > 0) {
        z->flags |= ZSTREAM_FLAG_IN_STREAM;
```

- err = Z_OK;   break;   }

I think Eric (a.k.a drbrain) should have any idea, so I'll assign this ticket to him.

thakns,

#2 - 10/08/2012 12:29 AM - nagachika (Tomoyuki Chikanaga)

- File zlib_inflate_buf_error.patch added

- Category changed from core to ext

- Assignee changed from drbrain (Eric Hodel) to nagachika (Tomoyuki Chikanaga)

Hello,

I've investigated this little more deeper.

If inflate() (aka z->func->run()) return under condition which z->stream.avail_in == z->stream.avail_out == 0, current zstream_run_func() call inflate() once more even though there's no input available. In that case inflate() return Z_BUF_ERROR.

However, deflate() have hidden input buffer in z->stream.state (opaque structure) and should be called even when z->stream.avail_in == 0 (while z->stream.avail_out == 0).

I think zstream_run_func() should break from while loop when zstream->avail_in == 0 only if z->func->run == inflate.

I will commit an attached patch tomorrow if there's no objection.

ruby-dev □□□□□□□□□

□□□□□□□□□□□□

zstream_run_func() □ inflate() (z->func->run()) □□□□□□□□□□□□□□□□□□□/□□□□□□ (z->stream.avail_in == z->stream.avail_out == 0)
□□□□□□□□□□□□□□□□□□□□□□□□□□ inflate() □□□□□□□□□□zlib □□□□□□□□□□□ inflate() □□□□ Z_BUF_ERROR □□□□□□□□

□□ deflate() □□□□□□□□ z->stream->state □□□□□□□□□□□□□□□□□□□□□□□□z->stream.avail_in == 0 □□□□□□ deflate() □□□□□□□□□□□□□□□□□□

□□□□□□□□□□□ z->func->run □ inflate □□□□□ z->stream.avail_in == 0 □□□□ zstream_run_func() □ while □□□□□□□□□□□□ inflate()
(z->func->run())□□□□□□□□□□□□□□□□□□□□ make test-all □□□□□□□□□□□□□□
□□□ gem □□

#3 - 10/09/2012 01:40 AM - nagachika (Tomoyuki Chikanaga)

- Status changed from Open to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r37119.

Hiroshi, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- ext/zlib/zlib.c (zstream_run_func): don't call inflate() when z->stream.avail_in == 0. it return Z_BUF_ERROR. but deflate() could be called with z->stream->avail_in == 0 because it has hidden buffer in z->stream->state (opaque structure). fix for gem install error. [ruby-dev:46149] [Bug #7040]

Files

zlib_inflate_buf_error.patch	634 Bytes	10/08/2012	nagachika (Tomoyuki Chikanaga)