Rewinding and iterating through gzipped IO leads to segmentation fault

06/01/2013 12:15 AM - vicente.mundim (Vicente Mundim)

Status: Closed
Priority: Normal
Assignee: nagachika (Tomoyuki Chikanaga)

Description
The following steps reproduce the bug in 2.0.0:

- Create a file and gzip it in a terminal:
  
  ```
  echo "some content" > compressed_file && gzip compressed_file
  ```

Then start a IRB session with the following code:

```ruby
require 'zlib'
filename = "compressed_file.gz"
io = Zlib::GzipReader.new(open(filename, 'rb'))
io.rewind
io.each {} # segmentation_fault in Ruby 2.0.0
```

This works in Ruby 1.9.3, 1.9.2, and 1.8.7.

Associated revisions

Revision aa8cc01a - 05/31/2013 11:00 PM - nobu (Nobuyoshi Nakada)

zlib.c: check EOF

- ext/zlib/zlib.c (gzfile_read, gzfile_read_all, gzfile_getc), (gzreader_gets): check EOF. [ruby-core:55220] [Bug #8467]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@41014 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 41014 - 05/31/2013 11:00 PM - nobu (Nobuyoshi Nakada)

zlib.c: check EOF

- ext/zlib/zlib.c (gzfile_read, gzfile_read_all, gzfile_getc), (gzreader_gets): check EOF. [ruby-core:55220] [Bug #8467]

Revision 41014 - 05/31/2013 11:00 PM - nobu (Nobuyoshi Nakada)

zlib.c: check EOF

- ext/zlib/zlib.c (gzfile_read, gzfile_read_all, gzfile_getc), (gzreader_gets): check EOF. [ruby-core:55220] [Bug #8467]

Revision 41014 - 05/31/2013 11:00 PM - nobu (Nobuyoshi Nakada)

zlib.c: check EOF

- ext/zlib/zlib.c (gzfile_read, gzfile_read_all, gzfile_getc), (gzreader_gets): check EOF. [ruby-core:55220] [Bug #8467]

Revision 41014 - 05/31/2013 11:00 PM - nobu (Nobuyoshi Nakada)

zlib.c: check EOF

- ext/zlib/zlib.c (gzfile_read, gzfile_read_all, gzfile_getc), (gzreader_gets): check EOF. [ruby-core:55220] [Bug #8467]

Revision 41014 - 05/31/2013 11:00 PM - nobu (Nobuyoshi Nakada)

zlib.c: check EOF

- ext/zlib/zlib.c (gzfile_read, gzfile_read_all, gzfile_getc), (gzreader_gets): check EOF. [ruby-core:55220] [Bug #8467]
zlib.c: check EOF

- ext/zlib/zlib.c (gzfile_read, gzfile_read_all, gzfile_getc), (gzreader_gets): check EOF. [ruby-core:55220] [Bug #8467]

Revision cc94db60 - 06/04/2013 03:44 PM - nagachika (Tomoyuki Chikanaga)
merge revision(s) 41014: [Backport #8467]

* ext/zlib/zlib.c (gzfile_read, gzfile_read_all, gzfile_getc), (gzreader_gets): check EOF. [ruby-core:55220] [Bug #8467]
* ext/zlib/zlib.c (gzfile_read, gzfile_read_all, gzfile_getc), (gzreader_gets): check EOF. [ruby-core:55220] [Bug #8467]
* lib/cgi/util.rb: All class methods moduleized.

History

#1 - 06/01/2013 08:00 AM - nobu (Nobuyoshi Nakada)
- Status changed from Open to Closed
- % Done changed from 0 to 100

This issue was solved with changeset r41014.
Vicente, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

zlib.c: check EOF

- ext/zlib/zlib.c (gzfile_read, gzfile_read_all, gzfile_getc), (gzreader_gets): check EOF. [ruby-core:55220] [Bug #8467]

#2 - 06/01/2013 08:01 AM - nobu (Nobuyoshi Nakada)
- Backport changed from 1.9.3: UNKNOWN, 2.0.0: UNKNOWN to 2.0.0: REQUIRED

#3 - 06/01/2013 11:54 AM - nagachika (Tomoyuki Chikanaga)
- Tracker changed from Bug to Backport
- Project changed from Ruby master to Backport200
- Category deleted (lib)
- Status changed from Closed to Assigned
- Assignee set to nagachika (Tomoyuki Chikanaga)

#4 - 06/05/2013 12:45 AM - nagachika (Tomoyuki Chikanaga)
- Status changed from Assigned to Closed

This issue was solved with changeset r41073.
Vicente, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

merge revision(s) 41014: [Backport #8467]
* ext/zlib/zlib.c (gzfile_read, gzfile_read_all, gzfile_getc),
  (gzreader_gets): check EOF. [ruby-core:55220] [Bug #8467]

* ext/zlib/zlib.c (gzfile_read, gzfile_read_all, gzfile_getc),
  (gzreader_gets): check EOF. [ruby-core:55220] [Bug #8467]

* lib/cgi/util.rb: All class methods moduleized.

Files
---
<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>zlib_bug.rb</td>
<td>152 Bytes</td>
<td>06/01/2013</td>
<td>vicente.mundim (Vicente Mundim)</td>
</tr>
<tr>
<td>ruby_2013-05-31-121414_vm-imac.crash</td>
<td>8.99 KB</td>
<td>06/01/2013</td>
<td>vicente.mundim (Vicente Mundim)</td>
</tr>
</tbody>
</table>