

Backport191 - Bug #3189

[BUG] Segmentation fault

04/23/2010 05:19 AM - brettkd (Brett Dawkins)

Status:	Open
Priority:	Normal
Assignee:	
Target version:	
ruby -v:	ruby 1.9.1p376

Description

```
=begin
running the command bundle install with rails3.0.0.beta2, ruby 1.9.1p376, ubuntu 9.10

/usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package/tar_input.rb:212: [BUG] Segmentation fault
ruby 1.9.1p376 (2009-12-07 revision 26041) [i686-linux]

-- control frame -----
c:0047 p:---- s:0210 b:0210 l:000209 d:000209 CFUNC :inflate
c:0046 p:0147 s:0206 b:0205 l:000204 d:000204 METHOD /usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package/tar_input.rb:212
c:0045 p:0034 s:0198 b:0198 l:000177 d:000197 BLOCK /usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package/tar_input.rb:122
c:0044 p:0114 s:0194 b:0194 l:000180 d:000193 BLOCK /usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package/tar_reader.rb:63
c:0043 p:---- s:0186 b:0186 l:000185 d:000185 FINISH
c:0042 p:---- s:0184 b:0184 l:000183 d:000183 CFUNC :loop
c:0041 p:0011 s:0181 b:0181 l:000180 d:000180 METHOD /usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package/tar_reader.rb:54
c:0040 p:0012 s:0178 b:0178 l:000177 d:000177 METHOD /usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package/tar_input.rb:120
c:0039 p:0046 s:0174 b:0174 l:001504 d:0012e0 BLOCK /usr/local/lib/ruby/site_ruby/1.9.1/rubygems/format.rb:67
c:0038 p:0027 s:0171 b:0171 l:000170 d:000170 METHOD /usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package/tar_input.rb:19
c:0037 p:0095 s:0164 b:0164 l:000163 d:000163 METHOD /usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package.rb:55
c:0036 p:0045 s:0156 b:0156 l:001504 d:001504 METHOD /usr/local/lib/ruby/site_ruby/1.9.1/rubygems/format.rb:63
c:0035 p:0018 s:0149 b:0149 l:000138 d:000148 BLOCK /usr/local/lib/ruby/site_ruby/1.9.1/rubygems/format.rb:51
c:0034 p:---- s:0146 b:0146 l:000145 d:000145 FINISH
c:0033 p:---- s:0144 b:0144 l:000143 d:000143 CFUNC :open
c:0032 p:0186 s:0139 b:0139 l:000138 d:000138 METHOD /usr/local/lib/ruby/site_ruby/1.9.1/rubygems/format.rb:50
c:0031 p:0020 s:0132 b:0132 l:000122 d:000131 BLOCK
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/source.rb:139
c:0030 p:---- s:0128 b:0128 l:000127 d:000127 FINISH
c:0029 p:---- s:0126 b:0126 l:000125 d:000125 CFUNC :each
c:0028 p:0059 s:0123 b:0123 l:000122 d:000122 METHOD
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/source.rb:138
c:0027 p:0031 s:0119 b:0119 l:000118 d:000118 METHOD /usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/index.rb:43
c:0026 p:0056 s:0115 b:0115 l:000114 d:000114 METHOD /usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/index.rb:34
c:0025 p:0012 s:0111 b:0110 l:000102 d:000109 BLOCK /usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/index.rb:26
c:0024 p:0020 s:0107 b:0107 l:000106 d:000106 METHOD /usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/index.rb:5
c:0023 p:0011 s:0103 b:0103 l:000102 d:000102 METHOD /usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/index.rb:25
c:0022 p:0037 s:0100 b:0099 l:000091 d:000098 BLOCK
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/environment.rb:15
c:0021 p:0020 s:0096 b:0096 l:000095 d:000095 METHOD /usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/index.rb:5
c:0020 p:0030 s:0092 b:0092 l:000091 d:000091 METHOD
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/environment.rb:13
c:0019 p:0014 s:0089 b:0087 l:000086 d:000086 METHOD
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/environment.rb:59
c:0018 p:0024 s:0084 b:0084 l:000083 d:000083 METHOD
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/environment.rb:28
c:0017 p:0071 s:0081 b:0081 l:000080 d:000080 METHOD
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/runtime.rb:85
c:0016 p:0023 s:0077 b:0077 l:000076 d:000076 METHOD /usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/cli.rb:138
c:0015 p:0315 s:0073 b:0073 l:000072 d:000072 METHOD /usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/cli.rb:91
c:0014 p:0036 s:0067 b:0067 l:000066 d:000066 METHOD
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/vendor/thor/task.rb:33
c:0013 p:0058 s:0061 b:0061 l:000d78 d:000060 BLOCK
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/vendor/thor/invocation.rb:109
c:0012 p:---- s:0056 b:0056 l:000055 d:000055 FINISH
```

```
c:0011 p:---- s:0054 b:0054 l:000053 d:000053 CFUNC :call
c:0010 p:0227 s:0049 b:0049 l:000d78 d:000d78 METHOD
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/vendor/thor/invoke.rb:116
c:0009 p:0224 s:0035 b:0035 l:000020 d:000034 BLOCK
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/vendor/thor.rb:137
c:0008 p:0093 s:0027 b:0027 l:000026 d:000026 METHOD
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/vendor/thor/base.rb:378
c:0007 p:0027 s:0021 b:0021 l:000020 d:000020 METHOD
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/vendor/thor.rb:124
c:0006 p:0054 s:0016 b:0016 l:000015 d:000015 TOP /usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/bin/bundle:13
c:0005 p:---- s:0013 b:0013 l:000012 d:000012 FINISH
c:0004 p:---- s:0011 b:0011 l:000010 d:000010 CFUNC :load
c:0003 p:0127 s:0007 b:0007 l:0004ac d:001e10 EVAL /usr/local/bin/bundle:19
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:0004ac d:0004ac TOP
```

-- Ruby level backtrace information-----

```
/usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package/tar_input.rb:212:in inflate'
/usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package/tar_input.rb:212:in zip_stream'
/usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package/tar_input.rb:122:in block in each'
/usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package/tar_reader.rb:63:in block in each'
/usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package/tar_reader.rb:54:in loop'
/usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package/tar_reader.rb:54:in each'
/usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package/tar_input.rb:120:in each'
/usr/local/lib/ruby/site_ruby/1.9.1/rubygems/format.rb:67:in block in from_io'
/usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package/tar_input.rb:19:in open'
/usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package.rb:55:in open'
/usr/local/lib/ruby/site_ruby/1.9.1/rubygems/format.rb:63:in from_io'
/usr/local/lib/ruby/site_ruby/1.9.1/rubygems/format.rb:51:in block in from_file_by_path'
/usr/local/lib/ruby/site_ruby/1.9.1/rubygems/format.rb:50:in open'
/usr/local/lib/ruby/site_ruby/1.9.1/rubygems/format.rb:50:in from_file_by_path'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/source.rb:139:in block in specs'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/source.rb:138:in each'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/source.rb:138:in specs'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/index.rb:43:in from_cached_specs'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/index.rb:34:in application_cached_gems'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/index.rb:26:in block in cached_gems'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/index.rb:5:in build'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/index.rb:25:in cached_gems'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/environment.rb:15:in block in index'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/index.rb:5:in build'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/environment.rb:13:in index'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/environment.rb:59:in resolve_locally'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/environment.rb:28:in specs'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/runtime.rb:85:in cache'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/cli.rb:138:in cache'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/cli.rb:91:in install'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/vendor/thor/task.rb:33:in run'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/vendor/thor/invoke.rb:109:in block in invoke'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/vendor/thor/invoke.rb:116:in call'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/vendor/thor/invoke.rb:116:in invoke'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/vendor/thor.rb:137:in block in start'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/vendor/thor/base.rb:378:in start'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/lib/bundler/vendor/thor.rb:124:in start'
/usr/local/lib/ruby/gems/1.9.1/gems/bundler-0.9.16/bin/bundle:13:in
/usr/local/bin/bundle:19:in load'
/usr/local/bin/bundle:19:in
```

-- C level backtrace information -----

```
0x81239d7 /usr/local/bin/ruby(rb_vm_bugreport+0x47) [0x81239d7]
0x8150343 /usr/local/bin/ruby [0x8150343]
0x81503b8 /usr/local/bin/ruby(rb_bug+0x28) [0x81503b8]
0x80d33a8 /usr/local/bin/ruby [0x80d33a8]
0xb7766410 [0xb7766410]
0xb7604349 /lib/tls/i686/cmox/libc.so.6 [0xb7604349]
0xb760485d /lib/tls/i686/cmox/libc.so.6(realloc+0xdd) [0xb760485d]
```

```
0x8065241 /usr/local/bin/ruby(ruby_xrealloc+0x31) [0x8065241]
0x80e53f8 /usr/local/bin/ruby(rb_str_resize+0x1a8) [0x80e53f8]
0xb7499ca5 /usr/local/lib/ruby/1.9.1/i686-linux/zlib.so [0xb7499ca5]
0xb749a346 /usr/local/lib/ruby/1.9.1/i686-linux/zlib.so [0xb749a346]
0xb749b239 /usr/local/lib/ruby/1.9.1/i686-linux/zlib.so [0xb749b239]
0xb749bb2f /usr/local/lib/ruby/1.9.1/i686-linux/zlib.so [0xb749bb2f]
0x8113770 /usr/local/bin/ruby [0x8113770]
0x811e8cd /usr/local/bin/ruby [0x811e8cd]
0x811854d /usr/local/bin/ruby [0x811854d]
0x811b3a6 /usr/local/bin/ruby [0x811b3a6]
0x811c9f6 /usr/local/bin/ruby [0x811c9f6]
0x805cdd1 /usr/local/bin/ruby(rb_rescue2+0x141) [0x805cdd1]
0x8114d7b /usr/local/bin/ruby [0x8114d7b]
0x8113770 /usr/local/bin/ruby [0x8113770]
0x811e8cd /usr/local/bin/ruby [0x811e8cd]
0x811854d /usr/local/bin/ruby [0x811854d]
0x811b3a6 /usr/local/bin/ruby [0x811b3a6]
0x812075a /usr/local/bin/ruby(rb_yield+0x1aa) [0x812075a]
0x805caf1 /usr/local/bin/ruby(rb_ensure+0x81) [0x805caf1]
0x806bd97 /usr/local/bin/ruby [0x806bd97]
0x807639d /usr/local/bin/ruby [0x807639d]
0x811343d /usr/local/bin/ruby [0x811343d]
0x8113770 /usr/local/bin/ruby [0x8113770]
0x811e8cd /usr/local/bin/ruby [0x811e8cd]
0x811854d /usr/local/bin/ruby [0x811854d]
0x811b3a6 /usr/local/bin/ruby [0x811b3a6]
0x812075a /usr/local/bin/ruby(rb_yield+0x1aa) [0x812075a]
0x812e171 /usr/local/bin/ruby(rb_ary_each+0x41) [0x812e171]
0x8113770 /usr/local/bin/ruby [0x8113770]
0x811e8cd /usr/local/bin/ruby [0x811e8cd]
0x811854d /usr/local/bin/ruby [0x811854d]
0x811b3a6 /usr/local/bin/ruby [0x811b3a6]
0x811dbc0 /usr/local/bin/ruby(rb_vm_invoke_proc+0x260) [0x811dbc0]
0x805fcc4 /usr/local/bin/ruby [0x805fcc4]
0x811343d /usr/local/bin/ruby [0x811343d]
0x8113770 /usr/local/bin/ruby [0x8113770]
0x811e8cd /usr/local/bin/ruby [0x811e8cd]
0x811854d /usr/local/bin/ruby [0x811854d]
0x811b3a6 /usr/local/bin/ruby [0x811b3a6]
0x811b6f9 /usr/local/bin/ruby(rb_iseq_eval+0xf9) [0x811b6f9]
0x815126a /usr/local/bin/ruby(rb_load+0x16a) [0x815126a]
0x8151399 /usr/local/bin/ruby [0x8151399]
0x811343d /usr/local/bin/ruby [0x811343d]
0x8113770 /usr/local/bin/ruby [0x8113770]
0x811e8cd /usr/local/bin/ruby [0x811e8cd]
0x811854d /usr/local/bin/ruby [0x811854d]
0x811b3a6 /usr/local/bin/ruby [0x811b3a6]
0x811b5d9 /usr/local/bin/ruby(rb_iseq_eval_main+0x99) [0x811b5d9]
0x805d62f /usr/local/bin/ruby(ruby_exec_node+0x9f) [0x805d62f]
0x805e9c6 /usr/local/bin/ruby(ruby_run_node+0x46) [0x805e9c6]
0x805c07a /usr/local/bin/ruby(main+0x5a) [0x805c07a]
0xb75aab56 /lib/tls/i686/cmov/libc.so.6(__libc_start_main+0xe6) [0xb75aab56]
0x805bf81 /usr/local/bin/ruby [0x805bf81]
```

[NOTE]

You may encounter a bug of Ruby interpreter. Bug reports are welcome.

For details: <http://www.ruby-lang.org/bugreport.html>

=end

History

#1 - 04/23/2010 07:38 AM - matz (Yukihiro Matsumoto)

=begin

Hi,

In message "Re: [ruby-core:29738] [Bug #3189] [BUG] Segmentation fault"
on Fri, 23 Apr 2010 05:19:10 +0900, Brett Dawkins redmine@ruby-lang.org writes:

|Author: Brett Dawkins
|Status: Open, Priority: Normal
|ruby -v: ruby 1.9.1p376

|
|running the command bundle install with rails3.0.0.beta2, ruby 1.9.1p376, ubuntu 9.10

|
|/usr/local/lib/ruby/site_ruby/1.9.1/rubygems/package/tar_input.rb:212: [BUG] Segmentation fault
|ruby 1.9.1p376 (2009-12-07 revision 26041) [i686-linux]

Your bug have very few chance to be fixed without reproducing string/input. Note that most of core developers are NOT using rails, so you have describe detailed steps to reproduce the problem.

```
matz.
```

=end