

Ruby - Bug #1329

Ruby 1.8.8 "p eval('0' + '+0.1*n)" Segmentation Fault

03/30/2009 05:58 AM - mrkn (Kenta Murata)

Status: Closed Priority: Normal Assignee: wyhaines (Kirk Haines) Target version: ruby -v: ruby 1.8.8dev (2009-03-19) [i386-darwin9.6.0]	Backport: 2.5: UNKNOWN, 2.6: UNKNOWN
Description =begin "p eval('0' + '+0.1*n)" n N1 N2 Segmentation Fault N1 N2 \$ ~/ruby-1.8.8-r23009/bin/ruby -ve "p eval('0'+'+0.1*4581)" ruby 1.8.8dev (2009-03-19) [i386-darwin9.6.0] 458.100000000036 \$ ~/ruby-1.8.8-r23009/bin/ruby -ve "p eval('0'+'+0.1*4582)" ruby 1.8.8dev (2009-03-19) [i386-darwin9.6.0] -e:1: can't modify frozen string (TypeError) \$ ~/ruby-1.8.8-r23009/bin/ruby -ve "p eval('0'+'+0.1*5132)" ruby 1.8.8dev (2009-03-19) [i386-darwin9.6.0] -e:1: can't modify frozen string (TypeError) \$ ~/ruby-1.8.8-r23009/bin/ruby -ve "p eval('0'+'+0.1*5133)" ruby 1.8.8dev (2009-03-19) [i386-darwin9.6.0] Segmentation fault eval eval TypeError SEGV \$ ~/ruby-1.8.8-r23009/bin/ruby -ve "'0'+'+0.1*5133" ruby 1.8.8dev (2009-03-19) [i386-darwin9.6.0] -e:1: warning: useless use of + in void context =end	

Associated revisions

Revision a1b9ce96e9ffcfa97e6b95817261f7af461c86c2 - 03/30/2009 03:12 AM - nobu (Nobuyoshi Nakada)

- eval.c (rb_eval): checks for interrupt, stack and finalizers too. [ruby-dev:38208], [Bug #1329]
- eval.c (eval): replaces the message if frozen.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_8@23096 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision a1b9ce96e9ffcfa97e6b95817261f7af461c86c2 - 03/30/2009 03:12 AM - nobu (Nobuyoshi Nakada)

- eval.c (rb_eval): checks for interrupt, stack and finalizers too. [ruby-dev:38208], [Bug #1329]
- eval.c (eval): replaces the message if frozen.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_8@23096 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision a1b9ce96 - 03/30/2009 03:12 AM - nobu (Nobuyoshi Nakada)

- `eval.c (rb_eval)`: checks for interrupt, stack and finalizers too. [ruby-dev:38208], [Bug #1329]
- `eval.c (eval)`: replaces the message if frozen.

git-svn-id: [svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_8@23096](https://ci.ruby-lang.org/ruby/branches/ruby_1_8@23096) b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 4b4ac8ac64ffaa6de94ac254ce1c6aea2b743269 - 07/06/2009 07:25 AM - shyouhei (Shyouhei Urabe)

merge revision(s) 23096:

- * eval.c (rb_eval): checks for interrupt, stack and finalizers too. [ruby-dev:38208], [Bug #1329]
- * eval.c (eval): replaces the message if frozen.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_8_7@23972 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 4b4ac8ac64ffaa6de94ac254ce1c6aea2b743269 - 07/06/2009 07:25 AM - shyouhei (Shyouhei Urabe)

merge revision(s) 23096:

- * eval.c (rb_eval): checks for interrupt, stack and finalizers too. [ruby-dev:38208], [Bug #1329]
- * eval.c (eval): replaces the message if frozen.

git-svn-id: [svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_8_7@23972](https://ci.ruby-lang.org/ruby/branches/ruby_1_8_7@23972) b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 4b4ac8ac - 07/06/2009 07:25 AM - shyouhei (Shyouhei Urabe)

merge revision(s) 23096:

- * eval.c (rb_eval): checks for interrupt, stack and finalizers too. [ruby-dev:38208], [Bug #1329]
- * eval.c (eval): replaces the message if frozen.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_8_7@23972 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 03/30/2009 10:53 AM - mrkn (Kenta Murata)

```
=begin
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
$ ~/ruby-1.8.8-r23088/bin/ruby -ve "p eval('0'++0.1**4581)"
ruby 1.8.8dev (2009-03-28) [i386-darwin9.6.0]
458.1000000000036
$ ~/ruby-1.8.8-r23088/bin/ruby -ve "p eval('0'++0.1**4582)"
ruby 1.8.8dev (2009-03-28) [i386-darwin9.6.0]
-e:1: can't modify frozen string (TypeError)
$ ~/ruby-1.8.8-r23088/bin/ruby -ve "p eval('0'++0.1**5132)"
ruby 1.8.8dev (2009-03-28) [i386-darwin9.6.0]
-e:1: can't modify frozen string (TypeError)
$ ~/ruby-1.8.8-r23088/bin/ruby -ve "p eval('0'++0.1**5133)"
ruby 1.8.8dev (2009-03-28) [i386-darwin9.6.0]
Segmentation fault
```

```
$ ~/ruby-1.8.8-r23088/bin/ruby -ve "'0'+'+0.1'*5133"
ruby 1.8.8dev (2009-03-28) [i386-darwin9.6.0]
-e:1: warning: useless use of + in void context
=end
```

#2 - 03/30/2009 12:17 PM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

- % Done changed from 0 to 100

```
=begin
Applied in changeset r23096.
=end
```

#3 - 05/12/2009 09:37 PM - shyouhei (Shyouhei Urabe)

- *Status changed from Closed to Open*
- *Assignee set to shyouhei (Shyouhei Urabe)*

=begin

=end

#4 - 07/06/2009 04:26 PM - shyouhei (Shyouhei Urabe)

- *Assignee changed from shyouhei (Shyouhei Urabe) to wyhaines (Kirk Haines)*

=begin

1.8.6 also has this problem.

=end

#5 - 09/14/2010 04:36 PM - shyouhei (Shyouhei Urabe)

- *Status changed from Open to Assigned*

=begin

=end

#6 - 08/27/2019 04:04 PM - jeremyevans0 (Jeremy Evans)

- *Tracker changed from Backport to Bug*
- *Project changed from 11 to Ruby*
- *Description updated*
- *Status changed from Assigned to Closed*
- *ruby -v set to ruby 1.8.8dev (2009-03-19) [i386-darwin9.6.0]*
- *Backport set to 2.5: UNKNOWN, 2.6: UNKNOWN*