

## Ruby 1.8 - Bug #3235

### Stack Traceback running irb on Linux

05/02/2010 09:25 PM - rubys (Sam Ruby)

<b>Status:</b>	Open
<b>Priority:</b>	Normal
<b>Assignee:</b>	
<b>Target version:</b>	Ruby 1.8.8
<b>ruby -v:</b>	ruby 1.8.8dev (2010-04-24) [x86_64-linux]

**Description**

```
=begin
Reproduction instructions:

Execute "irb" from the command line with no parameters.

Result:

*** glibc detected *** irb: realloc(): invalid next size: 0x081e5f50 ***
===== Backtrace: =====
/lib/tls/i686/cmov/libc.so.6[0xb7651803]
/lib/tls/i686/cmov/libc.so.6(realloc+0x10b)[0xb765375b]
irb(ruby_xrealloc+0x56)[0x8075646]

Full backtrace can be seen here:

http://intertwingly.net/projects/AWDwR3/checkdepot-188/section-19.html

Regression was introduced by:

http://redmine.ruby-lang.org/repositories/diff/ruby-18/lib/cgi.rb?rev=r27468
=end
```

### History

#### #1 - 05/02/2010 10:40 PM - rubys (Sam Ruby)

```
=begin
Correction: regression was introduced by:

http://redmine.ruby-lang.org/repositories/diff/ruby-18/?rev=27468
```

Ruby revision 27466 works.  
=end

#### #2 - 05/03/2010 05:25 PM - nobu (Nobuyoshi Nakada)

```
=begin
Hi,
```

At Sun, 2 May 2010 21:25:10 +0900,  
Sam Ruby wrote in [ruby-core:29934]:

Reproduction instructions:

Execute "irb" from the command line with no parameters.

Seems running with scripts according to your backtrace.  
I can't reproduce it on i686-linux and x86\_64-linux without  
parameters.

```
--
Nobu Nakada
```

```
=end
```

### #3 - 05/03/2010 07:38 PM - rubys (Sam Ruby)

- File *backtrace* added

=begin

I'm uploading a new backtrace that is running straight from the command line.

I am using rvm. For the backtrace I've provided, I've unset all environment variables that mention rvm (including IRBRC) *except* PATH. I've appended my environment variables at the end of the backtrace.

=end

### #4 - 05/29/2010 06:05 PM - rubyjedi (Laurence Lee)

- File *ruby\_envspace.patch* added

=begin

This bug manifests itself on Fedora 12, x64 architecture. The root cause is the environment space not being contiguous.

Attached is a patch that corrects this issue. Chances are good the same root cause can also affect Ruby 1.9.2-head.

=end

#### Files

---

backtrace	9.15 KB	05/03/2010	rubys (Sam Ruby)
ruby_envspace.patch	1.04 KB	05/29/2010	rubyjedi (Laurence Lee)