

Ruby - Bug #3851

Ruby 1.9.2p0 crash on filename with '['

09/20/2010 11:20 AM - jlambert (Jon Lambert)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:		
Description		Backport:
<pre>=begin On Windows Vista using ruby one-click installer. ruby 1.9.2p0 (2010-08-18) [i386-mingw32] If you have a left bracket in the file name, ruby crashes Example: ruby s[s Windows event info: Faulting application ruby.exe, version 1.9.2.0, time stamp 0x4c6d7c5e, faulting module msvcr7-ruby191.dll, version 1.9.2.0, time stamp 0x4c6d7c5e, exception code 0xc0000005, fault offset 0x0004f601, process id 0xa08, application start time 0x01cb5865dfb1d879. =end</pre>		

History

#1 - 09/20/2010 12:05 PM - luislavena (Luis Lavena)

```
=begin
Using quotes or not around the filename, it still crashes.

trunk does too.

1.8.7 does not:

    type "s[s"
    puts "hi"

    ruby -v "s[s"
    ruby 1.8.7 (2010-08-16 patchlevel 302) [i386-mingw32]
    hi

=end
```

#2 - 09/20/2010 12:44 PM - zenspider (Ryan Davis)

```
=begin

On Sep 19, 2010, at 20:05 , Luis Lavena wrote:

    Issue #3851 has been updated by Luis Lavena.

    Using quotes or not around the filename, it still crashes.

    trunk does too.

    1.8.7 does not:

        type "s[s"
        puts "hi"
```

```
ruby -v "s[s"
ruby 1.8.7 (2010-08-16 patchlevel 302) [i386-mingw32]
hi
```

This doesn't reproduce on OSX. If I had to guess, prolly not on any unix/linux.

Passed: 1.9.2-p0, 1.9.1-p129, 1.8.6-p399, 1.8.7-p302

=end

#3 - 09/20/2010 12:49 PM - luislavena (Luis Lavena)

=begin

On Mon, Sep 20, 2010 at 12:43 AM, Ryan Davis ryand-ruby@zenspider.com wrote:

This doesn't reproduce on OSX. If I had to guess, prolly not on any unix/linux.

Passed: 1.9.2-p0, 1.9.1-p129, 1.8.6-p399, 1.8.7-p302

Nor on Linux, this seems strictly related to argument parsing on Windows as this works:

```
ruby -I. -ve "load 's[s"
ruby 1.9.2p0 (2010-08-18) [i386-mingw32]
hi
```

--

Luis Lavena AREA 17

Perfection in design is achieved not when there is nothing more to add,
but rather when there is nothing more to take away.
Antoine de Saint-Exupéry

=end

#4 - 09/20/2010 02:26 PM - phasis68 (Heesob Park)

=begin

I think this must be a bug.

Here is a patch for the trunk:

```
--- dir.c      2010-09-20 14:12:13.000000000 +0900
+++ dir.c.new  2010-09-20 14:12:56.000000000 +0900
@@ -120,6 +120,7 @@
if (!*t1)
return NULL;
p = t1 + (r = rb_enc_mbclen(t1, pend, enc));
```

- ```
if (p[0] == '-' && p[1] != ']') {
 const char *t2 = p + 1;
 int r2;
```

=end

### #5 - 09/20/2010 06:13 PM - jlambert (Jon Lambert)

=begin

I actually ran across the problem by mistyping.

rspec spec/ as rspec s[ec/

```
ruby [foo
crash
```

```
ruby fo[
```

ruby: No such file or directory -- fo[ (LoadError)

ruby fo[o  
ruby: No such file or directory -- fo[o (LoadError)

ruby a[o  
crash

ruby f[o  
ruby: No such file or directory -- f[o (LoadError)

ruby foo[bar  
ruby: No such file or directory -- foo[bar (LoadError)

Seems to happen if [ is in positions 1 or 2 and follows particular characters like s or a as above.  
Encoding issue?

=end

**#6 - 09/20/2010 11:27 PM - nobu (Nobuyoshi Nakada)**

- *Status changed from Open to Closed*

- *% Done changed from 0 to 100*

=begin

This issue was solved with changeset r29306.

Jon, thank you for reporting this issue.

Your contribution to Ruby is greatly appreciated.

May Ruby be with you.

=end