Ruby master - Bug #3668
make check segfault in test_syntax.rb
08/09/2010 05:10 AM - luislavena (Luis Lavena)

Status: Closed
Priority: Normal
Assignee: nobu (Nobuyoshi Nakada)
Target version: 2.0
ruby -v: ruby 1.8.7 (2010-06-23 patchlevel 299) [i386-mingw32]

Description
=begin
While build Ruby 1.9.3dev (trunk) under MinGW (GCC 4.5.0) and running tests, it segfault with the following traceback:

C:/Users/Luis/Projects/oss/ruby/test/ruby/test_syntax.rb:18: [BUG] Segmentation fault
ruby 1.9.3dev (2010-08-08 trunk 28909) [i386-mingw32]

-- control frame ----------
c:0020 p:---- s:0082 b:0082 l:000081 d:000081 CFUNC  :read
c:0018 p:---- s:0073 b:0073 l:000072 d:000072 FINISH
c:0017 p:---- s:0071 b:0071 l:000070 d:000070 CFUNC  :each
c:0012 p:0091 s:0046 b:0046 l:000045 BLOCK C:/Users/Luis/Projects/oss/ruby/lib/minitest/unit.rb:641
c:0011 p:---- s:0041 b:0041 l:000040 d:000040 FINISH
c:0010 p:---- s:0039 b:0039 l:000038 d:000038 CFUNC  :each
  c:0009 p:0026 s:0036 b:0036 l:000035 BLOCK C:/Users/Luis/Projects/oss/ruby/lib/minitest/unit.rb:635
c:0008 p:---- s:0033 b:0033 l:000032 d:000032 FINISH
  c:0006 p:0028 s:0028 b:0028 l:000032c d:000032c METHOD C:/Users/Luis/Projects/oss/ruby/lib/test/unit/assertions.rb:34
  c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
  c:0001 p:0000 s:0002 b:0002 l:001dac d:001dac TOP

-- Ruby level backtrace information ****************************
  ../../../ruby/test/runner.rb:26:in <main>
  ../../../ruby/lib/test/unit.rb:21:in run
  ../../../ruby/lib/test/unit.rb:634:in run_test_suites
  ../../../ruby/lib/minitest/unit.rb:634:in each
  ../../../ruby/lib/minitest/unit.rb:635:inblock in run_test_suites
  ../../../ruby/lib/minitest/unit.rb:635:in each
  ../../../ruby/lib/minitest/unit.rb:641:inblock (2 levels) in run_test_suites
  ../../../ruby/lib/minitest/unit.rb:680:in run
  ../../../ruby/lib/test/test_syntax.rb:16:intest_syntax
  ../../../ruby/lib/test/test_syntax.rb:34:in assert_nothing_raised
  ../../../ruby/lib/test/test_syntax.rb:17:inblock in test_syntax
  ../../../ruby/lib/test/test_syntax.rb:17:in each
  ../../../ruby/lib/test/test_syntax.rb:18:inblock (2 levels) in test_syntax
  ../../../ruby/lib/test/test_syntax.rb:18:in "read"

Individual execution of the tests did not segfault, indicating that something executed before could have triggered it.

An error of a missing temporary extension and fail to load it was triggered as popup. Will try to execute tests again and see if can note the tests triggered the previous issue.

09/15/2021
Thank you.

History

#1 - 08/15/2010 04:26 AM - pweldon (Peter Weldon)
- File i386-mingw32.txt added
- File i386-mswin32_100.txt added

Appears to be triggered by heap corruption during test/ruby/test_string.rb. Likewise with [ruby 1.9.3dev (2010-08-15) [i386-mswin32_100]], heap corruption is detected when linked to the debug crt libs.

#2 - 08/16/2010 11:54 AM - usa (Usaku NAKAMURA)
- Status changed from Open to Assigned
- Assignee set to nobu (Nobuyoshi Nakada)

#3 - 08/17/2010 06:29 AM - pweldon (Peter Weldon)
- File string.c.bug3668.patch added

Seems to be a buffer overrun caused by changes in string.c (str_make_independent_expand) at r28863.
Patch attached.

Before patch:

```
ruby.exe --version
ruby 1.9.3dev (2010-08-16) [i386-mswin32_100]
```

```
ruby test/ruby/test_string.rb
Loaded suite test/ruby/test_string
Started
```

```
..........................
HEEL CORRUPTION DETECTED: after Normal block (#53951) at 0x022D5088.
..........................
Finished in 0.540031 seconds.
```

116 tests, 1771 assertions, 0 failures, 0 errors, 0 skips
Test run options: --seed 54485

#4 - 08/17/2010 07:47 AM - nobu (Nobuyoshi Nakada)
- Status changed from Assigned to Closed
- % Done changed from 0 to 100

This issue was solved with changeset r29018.
Luis, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

Files

<table>
<thead>
<tr>
<th>i386-mingw32.txt</th>
<th>2.93 KB</th>
<th>08/15/2010</th>
<th>pweldon (Peter Weldon)</th>
</tr>
</thead>
</table>

09/15/2021