Ruby trunk - Bug #14628

Misplaced colon causes segmentation fault

03/24/2018 07:24 AM - DavidEGrayson (David Grayson)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.5.0p0 (2017-12-25 revision 61468) [x86_64-linux]	**Backport:**	2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: UNKNOWN

Description

The following program with a misplaced colon causes a segmentation fault when you try to run it in Ruby 2.5.0p0 on both the Manjaro Linux and the MSYS2 platforms:

```
def a(x)
  case x
  when A
    :
  when B, C
  end
end
```

It also causes some spurious "dynamic constant assignment" error messages on the line after the misplaced colon. I wonder what's going on here! Seems like a parsing problem.

Here is a shell session from Linux demonstrating the issue:

```
$ ruby -v ast.rb
ruby 2.5.0p0 (2017-12-25 revision 61468) [x86_64-linux]
ast.rb:4: syntax error, unexpected ':'
    :
    ^
ast.rb:5: dynamic constant assignment
  when B, C
         ^
ast.rb:5: dynamic constant assignment
  when B, C
           ^
ast.rb: [BUG] Segmentation fault at 0x0000000000000020
ruby 2.5.0p0 (2017-12-25 revision 61468) [x86_64-linux]

-- Control frame information -----------------------------------------------
c:0001 p:0000 s:0003 E:0016f0 (none) [FINISH]


-- Machine register context ------------------------------------------------
 RIP: 0x00007fd4161d5cc8 RBP: 0x0000000000000000 RSP: 0x00007fff0db94a90
 RAX: 0x000055c278401390 RBX: 0x0000000000000020 RCX: 0x0000000000000001
 RDX: 0x0000000000028000 RDI: 0x000055c278401390 RSI: 0x000000000000291b
  R8: 0x0000000000000000  R9: 0x0000000000000000 R10: 0x000055c278401360
 R11: 0x0000000000000145 R12: 0x000055c278401360 R13: 0x00007fff0db95490
 R14: 0x00007fff0db94bee R15: 0x00007fff0db94dd8 EFL: 0x0000000000010202

-- C level backtrace information -------------------------------------------
/usr/lib/libruby.so.2.5(0x7fd4162a57a6) [0x7fd4162a57a6]
/usr/lib/libruby.so.2.5(0x7fd4162a59e1) [0x7fd4162a59e1]
/usr/lib/libruby.so.2.5(0x7fd41616be96) [0x7fd41616be96]
/usr/lib/libruby.so.2.5(0x7fd4162355e3) [0x7fd4162355e3]
/usr/lib/libc.so.6(0x7fd415d5b8e0) [0x7fd415d5b8e0]
/usr/lib/libruby.so.2.5(0x7fd4161d5cc8) [0x7fd4161d5cc8]
/usr/lib/libruby.so.2.5(0x7fd4161d6320) [0x7fd4161d6320]
/usr/lib/libruby.so.2.5(0x7fd4161e196c) [0x7fd4161e196c]
```

```
/usr/lib/libruby.so.2.5(0x7fd4161ed303) [0x7fd4161ed303]
/usr/lib/libruby.so.2.5(0x7fd4162a770d) [0x7fd4162a770d]
/usr/lib/libruby.so.2.5(rb_parser_compile_file_path+0x71) [0x7fd4161d9511]
/usr/lib/libruby.so.2.5(0x7fd416233859) [0x7fd416233859]
/usr/lib/libruby.so.2.5(rb_ensure+0xc3) [0x7fd416172293]
/usr/lib/libruby.so.2.5(0x7fd4162347db) [0x7fd4162347db]
/usr/lib/libruby.so.2.5(ruby_process_options+0x7a) [0x7fd416234d7a]
/usr/lib/libruby.so.2.5(ruby_options+0xbf) [0x7fd41617342f]
ruby(0x55c277b48898) [0x55c277b48898]
/usr/lib/libc.so.6(__libc_start_main+0xea) [0x7fd415d47f4a]
ruby(_start+0x2a) [0x55c277b488da]

-- Other runtime information -----------------------------------------------

* Loaded script: ast.rb

* Loaded features:

    0 enumerator.so
    1 thread.rb
    2 rational.so
    3 complex.so
    4 /usr/lib/ruby/2.5.0/x86_64-linux/enc/encdb.so
    5 /usr/lib/ruby/2.5.0/x86_64-linux/enc/trans/transdb.so
    6 /usr/lib/ruby/2.5.0/x86_64-linux/rbconfig.rb
    7 /usr/lib/ruby/2.5.0/rubygems/compatibility.rb
    8 /usr/lib/ruby/2.5.0/rubygems/defaults.rb
    9 /usr/lib/ruby/2.5.0/rubygems/deprecate.rb
   10 /usr/lib/ruby/2.5.0/rubygems/errors.rb
   11 /usr/lib/ruby/2.5.0/rubygems/version.rb
   12 /usr/lib/ruby/2.5.0/rubygems/requirement.rb
   13 /usr/lib/ruby/2.5.0/rubygems/platform.rb
   14 /usr/lib/ruby/2.5.0/rubygems/basic_specification.rb
   15 /usr/lib/ruby/2.5.0/rubygems/stub_specification.rb
   16 /usr/lib/ruby/2.5.0/rubygems/util/list.rb
   17 /usr/lib/ruby/2.5.0/x86_64-linux/stringio.so
   18 /usr/lib/ruby/2.5.0/uri/rfc2396_parser.rb
   19 /usr/lib/ruby/2.5.0/uri/rfc3986_parser.rb
   20 /usr/lib/ruby/2.5.0/uri/common.rb
   21 /usr/lib/ruby/2.5.0/uri/generic.rb
   22 /usr/lib/ruby/2.5.0/uri/ftp.rb
   23 /usr/lib/ruby/2.5.0/uri/http.rb
   24 /usr/lib/ruby/2.5.0/uri/https.rb
   25 /usr/lib/ruby/2.5.0/uri/ldap.rb
   26 /usr/lib/ruby/2.5.0/uri/ldaps.rb
   27 /usr/lib/ruby/2.5.0/uri/mailto.rb
   28 /usr/lib/ruby/2.5.0/uri.rb
   29 /usr/lib/ruby/2.5.0/rubygems/specification.rb
   30 /usr/lib/ruby/2.5.0/rubygems/exceptions.rb
   31 /usr/lib/ruby/2.5.0/rubygems/dependency.rb
   32 /usr/lib/ruby/2.5.0/rubygems/core_ext/kernel_gem.rb
   33 /usr/lib/ruby/2.5.0/monitor.rb
   34 /usr/lib/ruby/2.5.0/rubygems/core_ext/kernel_require.rb
   35 /usr/lib/ruby/2.5.0/rubygems.rb
   36 /usr/lib/ruby/2.5.0/rubygems/path_support.rb

* Process memory map:

55c277b48000-55c277b49000 r-xp 00000000 08:01 3156826                    /usr/bin/ruby
55c277d48000-55c277d49000 r--p 00000000 08:01 3156826                    /usr/bin/ruby
55c277d49000-55c277d4a000 rw-p 00001000 08:01 3156826                    /usr/bin/ruby
55c2782d0000-55c2786c7000 rw-p 00000000 00:00 0                          [heap]
7fd4144de000-7fd41478a000 r--s 00000000 08:01 3157631                    /usr/lib/libruby.so.2.5.0
7fd41478a000-7fd4147a0000 r-xp 00000000 08:01 3147514                    /usr/lib/libgcc_s.so.1
7fd4147a0000-7fd41499f000 ---p 00016000 08:01 3147514                    /usr/lib/libgcc_s.so.1
7fd41499f000-7fd4149a0000 r--p 00015000 08:01 3147514                    /usr/lib/libgcc_s.so.1
7fd4149a0000-7fd4149a1000 rw-p 00016000 08:01 3147514                    /usr/lib/libgcc_s.so.1
```

```
7fd4149de000-7fd4149e5000 r-xp 00000000 08:01 4072441                    /usr/lib/ruby/2.5.0/x86_6
4-linux/stringio.so
7fd4149e5000-7fd414be4000 ---p 00007000 08:01 4072441                    /usr/lib/ruby/2.5.0/x86_6
4-linux/stringio.so
7fd414be4000-7fd414be5000 r--p 00006000 08:01 4072441                    /usr/lib/ruby/2.5.0/x86_6
4-linux/stringio.so
7fd414be5000-7fd414be6000 rw-p 00007000 08:01 4072441                    /usr/lib/ruby/2.5.0/x86_6
4-linux/stringio.so
7fd414be6000-7fd414be8000 r-xp 00000000 08:01 7995751                    /usr/lib/ruby/2.5.0/x86_6
4-linux/enc/trans/transdb.so
7fd414be8000-7fd414de8000 ---p 00002000 08:01 7995751                    /usr/lib/ruby/2.5.0/x86_6
4-linux/enc/trans/transdb.so
7fd414de8000-7fd414de9000 r--p 00002000 08:01 7995751                    /usr/lib/ruby/2.5.0/x86_6
4-linux/enc/trans/transdb.so
7fd414de9000-7fd414dea000 rw-p 00003000 08:01 7995751                    /usr/lib/ruby/2.5.0/x86_6
4-linux/enc/trans/transdb.so
7fd414dea000-7fd414dec000 r-xp 00000000 08:01 7995702                    /usr/lib/ruby/2.5.0/x86_6
4-linux/enc/encdb.so
7fd414dec000-7fd414feb000 ---p 00002000 08:01 7995702                    /usr/lib/ruby/2.5.0/x86_6
4-linux/enc/encdb.so
7fd414feb000-7fd414fec000 r--p 00001000 08:01 7995702                    /usr/lib/ruby/2.5.0/x86_6
4-linux/enc/encdb.so
7fd414fec000-7fd414fed000 rw-p 00002000 08:01 7995702                    /usr/lib/ruby/2.5.0/x86_6
4-linux/enc/encdb.so
7fd414fed000-7fd4150ee000 rw-p 00000000 00:00 0
7fd4150ee000-7fd415239000 r-xp 00000000 08:01 3147210                    /usr/lib/libm-2.26.so
7fd415239000-7fd415438000 ---p 0014b000 08:01 3147210                    /usr/lib/libm-2.26.so
7fd415438000-7fd415439000 r--p 0014a000 08:01 3147210                    /usr/lib/libm-2.26.so
7fd415439000-7fd41543a000 rw-p 0014b000 08:01 3147210                    /usr/lib/libm-2.26.so
7fd41543a000-7fd415442000 r-xp 00000000 08:01 3147230                    /usr/lib/libcrypt-2.26.so
7fd415442000-7fd415642000 ---p 00008000 08:01 3147230                    /usr/lib/libcrypt-2.26.so
7fd415642000-7fd415643000 r--p 00008000 08:01 3147230                    /usr/lib/libcrypt-2.26.so
7fd415643000-7fd415644000 rw-p 00009000 08:01 3147230                    /usr/lib/libcrypt-2.26.so
7fd415644000-7fd415672000 rw-p 00000000 00:00 0
7fd415672000-7fd415675000 r-xp 00000000 08:01 3147211                    /usr/lib/libdl-2.26.so
7fd415675000-7fd415874000 ---p 00003000 08:01 3147211                    /usr/lib/libdl-2.26.so
7fd415874000-7fd415875000 r--p 00002000 08:01 3147211                    /usr/lib/libdl-2.26.so
7fd415875000-7fd415876000 rw-p 00003000 08:01 3147211                    /usr/lib/libdl-2.26.so
7fd415876000-7fd415908000 r-xp 00000000 08:01 3151224                    /usr/lib/libgmp.so.10.3.2
7fd415908000-7fd415b07000 ---p 00092000 08:01 3151224                    /usr/lib/libgmp.so.10.3.2
7fd415b07000-7fd415b08000 r--p 00091000 08:01 3151224                    /usr/lib/libgmp.so.10.3.2
7fd415b08000-7fd415b09000 rw-p 00092000 08:01 3151224                    /usr/lib/libgmp.so.10.3.2
7fd415b09000-7fd415b22000 r-xp 00000000 08:01 3147413                    /usr/lib/libpthread-2.26.
so
7fd415b22000-7fd415d21000 ---p 00019000 08:01 3147413                    /usr/lib/libpthread-2.26.
so
7fd415d21000-7fd415d22000 r--p 00018000 08:01 3147413                    /usr/lib/libpthread-2.26.
so
7fd415d22000-7fd415d23000 rw-p 00019000 08:01 3147413                    /usr/lib/libpthread-2.26.
so
7fd415d23000-7fd415d27000 rw-p 00000000 00:00 0
7fd415d27000-7fd415ed5000 r-xp 00000000 08:01 3147371                    /usr/lib/libc-2.26.so
7fd415ed5000-7fd4160d4000 ---p 001ae000 08:01 3147371                    /usr/lib/libc-2.26.so
7fd4160d4000-7fd4160d8000 r--p 001ad000 08:01 3147371                    /usr/lib/libc-2.26.so
7fd4160d8000-7fd4160da000 rw-p 001b1000 08:01 3147371                    /usr/lib/libc-2.26.so
7fd4160da000-7fd4160de000 rw-p 00000000 00:00 0
7fd4160de000-7fd416382000 r-xp 00000000 08:01 3157631                    /usr/lib/libruby.so.2.5.0
7fd416382000-7fd416581000 ---p 002a4000 08:01 3157631                    /usr/lib/libruby.so.2.5.0
7fd416581000-7fd416589000 r--p 002a3000 08:01 3157631                    /usr/lib/libruby.so.2.5.0
7fd416589000-7fd41658a000 rw-p 002ab000 08:01 3157631                    /usr/lib/libruby.so.2.5.0
7fd41658a000-7fd41659a000 rw-p 00000000 00:00 0
7fd41659a000-7fd4165bf000 r-xp 00000000 08:01 3147372                    /usr/lib/ld-2.26.so
7fd4165df000-7fd41677a000 r--p 00000000 08:01 3165555                    /usr/lib/locale/locale-ar
chive
7fd41677a000-7fd416781000 rw-p 00000000 00:00 0
7fd4167b7000-7fd4167b9000 r--s 00000000 08:01 3156826                    /usr/bin/ruby
7fd4167b9000-7fd4167ba000 ---p 00000000 00:00 0
```

```
7fd4167ba000-7fd4167be000 rw-p 00000000 00:00 0
7fd4167be000-7fd4167bf000 r--p 00024000 08:01 3147372                    /usr/lib/ld-2.26.so
7fd4167bf000-7fd4167c0000 rw-p 00025000 08:01 3147372                    /usr/lib/ld-2.26.so
7fd4167c0000-7fd4167c1000 rw-p 00000000 00:00 0
7fff0d39a000-7fff0db99000 rw-p 00000000 00:00 0                          [stack]
7fff0dbcc000-7fff0dbce000 r--p 00000000 00:00 0                          [vvar]
7fff0dbce000-7fff0dbd0000 r-xp 00000000 00:00 0                          [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0                  [vsyscall]


[NOTE]
You may have encountered a bug in the Ruby interpreter or extension libraries.
Bug reports are welcome.
For details: http://www.ruby-lang.org/bugreport.html

Aborted (core dumped)
```

Related issues:

Is duplicate of Ruby trunk - Bug #14261: invalid syntax segfaults: "x, true"	**Closed**

History

#1 - 03/24/2018 08:16 AM - shevegen (Robert A. Heiler)

Indeed, good find.

I believe the ruby parser is correct when it thinks it is a
constant, since it obviously is a constant (A, B, C).

However had, I think the ruby parser makes two mistakes:

(1) it assumes that there is a dynamic constant assignment
but I think this is wrong because there is no "=" and no
other way, in the above code, to assign a new constant
and its value (such as via Object.const_set()).

(2) I think it should not segfault in this case. even though
the input-code is obviously wrong.

The following code "works" in the sense that ruby does not segfault
but instead reports one correct error (it still is wrong about the
dynamic constant part:

```
def a(x)
  case x
  when A
  :
  when B, C:
  end
end

a(5)
```

Reports the very same error as:

```
def a(x)
  case x
  when A:
  when B, C:
  end
end

a(5)
```

So I don't think the ':' is the sole problem (odd that ruby
handles the second lack or existance of ':' different though.)

#2 - 03/24/2018 10:52 AM - nobu (Nobuyoshi Nakada)

- Is duplicate of Bug #14261: invalid syntax segfaults: "x, true" added

#3 - 03/24/2018 10:54 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

Thank you, that bug has been fixed already in the repository, and the next release will work fine.