

Ruby master - Bug #14620

Incorrect assignment causes segfault

03/20/2018 01:01 PM - samaaron (Sam Aaron)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.5.0p0 (2017-12-25 revision 61468) [x86_64-darwin17]	Backport:	2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: UNKNOWN

Description

The following code when executed on Ruby 2.5 causes a segfault on my machine (macOS High Sierra). This has been reproduced with a self-compiled Ruby as well as one from home-brew.

```
def foo
  puts 'hi'
end
```

```
foo, true
```

The segfault produced is as follows:

```
/Users/sam/tmp/ruby.rb:5: Can't assign to true
foo, true
  ^
```

```
/Users/sam/tmp/ruby.rb: [BUG] Segmentation fault at 0x0000000000000020
ruby 2.5.0p0 (2017-12-25 revision 61468) [x86_64-darwin17]
```

```
-- Crash Report log information -----
See Crash Report log file under the one of following:
* ~/Library/Logs/DiagnosticReports
* /Library/Logs/DiagnosticReports
for more details.
```

Don't forget to include the above Crash Report log file in bug reports.

```
-- Control frame information -----
c:0001 p:0000 s:0003 E:001000 (none) [FINISH]
```

```
-- Machine register context -----
rax: 0x00007fee536988a0 rbx: 0x00007fee53698870 rcx: 0x0000000000002a91b
rdx: 0x0000000000000000 rdi: 0x00007fee536988a0 rsi: 0x0000000000000291b
rbp: 0x00007ffef7db3420 rsp: 0x00007ffef7db3400 r8: 0x0000000000000000
r9: 0x0000000000000040 r10: 0x00007fff94f88040 r11: 0xffffffffffffffff
r12: 0x00007ffef7db4248 r13: 0x00007ffef7db486a r14: 0x0000000000000000
r15: 0x00007fee53698870 rip: 0x0000000107f09a44 rfl: 0x0000000000010202
```

```
-- C level backtrace information -----
```

```
0  libruby.2.5.dylib                0x0000000107fb8553 rb_print_backtrace + 29
1  libruby.2.5.dylib                0x0000000107fb8636 rb_vm_bugreport + 120
2  libruby.2.5.dylib                0x0000000107ea58f7 rb_bug_context + 206
3  libruby.2.5.dylib                0x0000000107f55d73 sig_do_nothing + 0
4  libsystem_platform.dylib        0x00007fff5c1d3f5a _sigtramp + 26
5  libruby.2.5.dylib                0x0000000107f09a44 list_append_gen + 62
6  libruby.2.5.dylib                0x0000000107f025e4 ruby_yyparse + 7970
7  libruby.2.5.dylib                0x0000000107f0d130 yycompile0 + 592
8  libruby.2.5.dylib                0x0000000107fb9338 rb_suppress_tracing + 212
9  libruby.2.5.dylib                0x0000000107f0c51e rb_parser_compile_file_path + 109
10 libruby.2.5.dylib                0x0000000107f52759 load_file_internal + 989
11 libruby.2.5.dylib                0x0000000107eaba3b rb_ensure + 194
12 libruby.2.5.dylib                0x0000000107f51e1d ruby_process_options + 2329
13 libruby.2.5.dylib                0x0000000107eaaaa1 ruby_options + 191
```

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

```
* Loaded script: /Users/sam/tmp/ruby.rb
```

```
* Loaded features:
```

```
 0 enumerator.so
 1 thread.rb
 2 rational.so
 3 complex.so
 4 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/x86_64-darwin17/enc/encdb.bundle
 5 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/x86_64-darwin17/enc/trans/transdb.bundle
 6 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/x86_64-darwin17/rbconfig.rb
 7 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/compatibility.rb
 8 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/defaults.rb
 9 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/deprecate.rb
10 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/errors.rb
11 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/version.rb
12 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/requirement.rb
13 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/platform.rb
14 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/basic_specification.rb
15 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/stub_specification.rb
16 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/util/list.rb
17 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/x86_64-darwin17/stringio.bundle
18 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/uri/rfc2396_parser.rb
19 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/uri/rfc3986_parser.rb
20 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/uri/common.rb
21 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/uri/generic.rb
22 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/uri/ftp.rb
23 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/uri/http.rb
24 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/uri/https.rb
25 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/uri/ldap.rb
26 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/uri/ldaps.rb
27 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/uri/mailto.rb
28 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/uri.rb
29 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/specification.rb
30 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/exceptions.rb
31 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/defaults/operating_system.rb
32 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/dependency.rb
33 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/core_ext/kernel_gem.rb
34 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/monitor.rb
35 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/core_ext/kernel_require.rb
36 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems.rb
37 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/rubygems/path_support.rb
38 /usr/local/lib/ruby/gems/2.5.0/gems/did_you_mean-1.2.0/lib/did_you_mean/version.rb
39 /usr/local/lib/ruby/gems/2.5.0/gems/did_you_mean-1.2.0/lib/did_you_mean/core_ext/name_error.
rb
40 /usr/local/lib/ruby/gems/2.5.0/gems/did_you_mean-1.2.0/lib/did_you_mean/levenshtein.rb
41 /usr/local/lib/ruby/gems/2.5.0/gems/did_you_mean-1.2.0/lib/did_you_mean/jaro_winkler.rb
42 /usr/local/lib/ruby/gems/2.5.0/gems/did_you_mean-1.2.0/lib/did_you_mean/spell_checker.rb
43 /usr/local/Cellar/ruby/2.5.0_2/lib/ruby/2.5.0/delegate.rb
44 /usr/local/lib/ruby/gems/2.5.0/gems/did_you_mean-1.2.0/lib/did_you_mean/spell_checkers/name_
error_checkers/class_name_checker.rb
45 /usr/local/lib/ruby/gems/2.5.0/gems/did_you_mean-1.2.0/lib/did_you_mean/spell_checkers/name_
error_checkers/variable_name_checker.rb
46 /usr/local/lib/ruby/gems/2.5.0/gems/did_you_mean-1.2.0/lib/did_you_mean/spell_checkers/name_
error_checkers.rb
47 /usr/local/lib/ruby/gems/2.5.0/gems/did_you_mean-1.2.0/lib/did_you_mean/spell_checkers/metho
d_name_checker.rb
48 /usr/local/lib/ruby/gems/2.5.0/gems/did_you_mean-1.2.0/lib/did_you_mean/spell_checkers/key_e
rror_checker.rb
49 /usr/local/lib/ruby/gems/2.5.0/gems/did_you_mean-1.2.0/lib/did_you_mean/spell_checkers/null_
checker.rb
50 /usr/local/lib/ruby/gems/2.5.0/gems/did_you_mean-1.2.0/lib/did_you_mean/formatters/plain_for
matter.rb
```

```
51 /usr/local/lib/ruby/gems/2.5.0/gems/did_you_mean-1.2.0/lib/did_you_mean.rb
```

[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>

[IMPORTANT]

Don't forget to include the Crash Report log file under
DiagnosticReports directory in bug reports.

Related issues:

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

Closed

History

#1 - 03/20/2018 02:52 PM - headius (Charles Nutter)

Actually just the last line is enough to cause the fault.

#2 - 03/20/2018 02:53 PM - nobu (Nobuyoshi Nakada)

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

#3 - 03/20/2018 02:54 PM - nobu (Nobuyoshi Nakada)

- *Status changed from Open to Closed*

- *Description updated*

Already fixed bug.