Ruby master - Bug #15400

Ruby 2.6.0 broken string literal assignment to a local variable in Dir.tmpdir

12/11/2018 06:48 PM - lamont (Lamont Granquist)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.6.0rc1 (2018-12-06 trunk 66253) [x86_64-darwin16]	**Backport:**	2.4: UNKNOWN, 2.5: UNKNOWN

Description

I think I've found a critical bug in ruby 2.6.0 unfortunately the failure condition is not easy to replicate or convert to a minimal example, or for me to even guess what the problem could be caused by.

To replicate:

```
git clone https://github.com/chef/chef.git
git checkout bc8ec91a66784d1deb4216913ccd89f440563b24
bundle install
bundle exec rspec ./spec/functional/http/simple_spec.rb
```

You should see 4 "ArgumentError: could not find a temporary directory" failures.

I've track the bug down to this line in Dir.tmpdir:

https://github.com/ruby/ruby/blob/10b96900b90914b0cc1dba36f9736c038db2859d/lib/tmpdir.rb#L31

changing that line to show debugging output:

```
pp dir
tmp = dir
pp tmp
```

Shows that dir is correctly set to "/var/folders/vl/7__gnv9x5sg745ntrsh0yglm0000gn/T/" while in the failing tests tmp remains nil after the assignment statement.

I can't explain how this could happen, or theorize what the bug could be.

The test suite itself is a complicated test which fires up a webrick server to act as a target host and then simulates a truncated download (more or less end-to-end rather than a unit test), which involves a timeout being forced to occur on the "server-side" in webrick to force the connection to get torn down, which should then cause the internal HTTP stack to determine that the download file size does not match the Content-Length in the HTTP header which then ultimately throws a custom exception back to the consumer of the library.

My guess is something to do with an exception being thrown in this process and some stack unwinding process is causing the internal state of this local variable to somehow be corrupted and that this local scratch space is being kept around in its corrupted state from call-to-call (the rest of the entire test suite, when run, goes completely off the rails at this point and floods the output with exceptions from Dir.tmpdir whenever it is used).

I don't think I'm using the JIT, I'm simply using ruby 2.6.0 installed from rvm. The bug replicates on both MacOS/Darwin and Ubuntu/Linux.

History

#1 - 12/11/2018 06:54 PM - lamont (Lamont Granquist)

Also I've replicated this failure on ruby-head as of a few minutes ago.

Based on the nature of the test, it is plausible that something is happening related to the 2.6.0 ruby changes to introduce the write_timeout -- but whatever is breaking the assignment of the string to a local variable seems more fundamental than that.

#2 - 12/11/2018 06:55 PM - lamont (Lamont Granquist)

- ruby -v changed from 2.6.0-rc1 to ruby 2.6.0rc1 (2018-12-06 trunk 66253) [x86_64-darwin16]

#3 - 12/12/2018 01:59 PM - ko1 (Koichi Sasada)

I can reproduce it on my environment and am debugging now.

#4 - 12/12/2018 02:32 PM - ko1 (Koichi Sasada)

- Status changed from Open to Third Party's Issue

I found a bug of webmock.

https://github.com/bblimke/webmock/pull/788

Not a ruby matter :p

#5 - 12/12/2018 05:47 PM - lamont (Lamont Granquist)

nice! thank you. that was a bizarre one.

#6 - 01/02/2019 06:25 PM - lamont (Lamont Granquist)

- Status changed from Third Party's Issue to Closed

this has been fixed in webmock and released in 3.5.1