Ruby master - Bug #14403

Crash and coredump (Stack consistency error) on ruby 2.5.0

01/25/2018 04:39 PM - jrochkind (jonathan rochkind)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.5.0p0 (2017-12-25 revision 61468) [x86_64-darwin16]	**Backport:**	2.3: DONTNEED, 2.4: DONTNEED, 2.5: DONE

Description

This reproduction script seems to make no sense, because it's extracted from an actual program where I encountered this bug, and trimmed down to be the minimal I can get to reproduce.

Parts of the script that seem irrelevant (like the if check that should never be true), if removed, remove the reproduction. This is why I'm glad I'm not a C programmer!

This executes without core dump on ruby 2.4.3p205 (2017-12-14 revision 61247) [x86_64-darwin16] -- runs fine, does not reproduce error, on 2.4.

I believe on ruby 2.5 it also reproduces on travis (which is where I originally encountered the problem), so I don't believe it is unique to the MacOS ruby build I am reporting here.

Console output at: https://gist.github.com/jrochkind/0e6ed450414f4577bdb886961e4d61ba

Crash report log file from ~/Library/Logs/DiagnosticReports/ruby_2018-01-25-113636_170220-C02T63QEFVH4.crash at: https://gist.github.com/jrochkind/6cbd60845cf36352491fb6d058ea2910

Related issues:

Is duplicate of Ruby master - Bug #14273: Stack Consistency Error from return...	**Closed**

History

#1 - 01/25/2018 04:40 PM - jrochkind (jonathan rochkind)

Oops, sorry, somehow missed reproduction script in the original report, here it is:

https://gist.github.com/jrochkind/a8344b1805badec8109b6f95c89a745b

```
require 'rexml/parsers/pullparser'

def look_at_record(parser)
  # While this first 'if' condition will never be triggered, it is somehow
  # neccesary as is to trigger the core dump.
  if Module.constants.index('FooBarBazNoSuchThing') && parser.is_a?(String)
  else
    while parser.has_next?
      event = parser.pull
      if event.end_element?
        if event[0] == "record"
          return "foo"
        end
      end
    end
  end
end


  sample_xml = <<EOF
<record>
  <leader>foo</leader>
</record>
EOF


parser = REXML::Parsers::PullParser.new(StringIO.new(sample_xml))
while parser.has_next?
```

```
  event = parser.pull
  # if it's the start of a record element
  if event.start_element? and event[0] == 'record'
    puts look_at_record(parser)
  end
end
```

#2 - 01/25/2018 11:52 PM - nobu (Nobuyoshi Nakada)

- Is duplicate of Bug #14273: Stack Consistency Error from return in loop added

#3 - 01/29/2018 07:51 AM - nomotch (kiyoshi nomo)

It is also reproduce in my environments.

```
sw_vers
ProductName:    Mac OS X
ProductVersion: 10.12.6
BuildVersion:   16G1212
```

```
ruby -v
ruby 2.5.0p0 (2017-12-25 revision 61467) [x86_64-darwin16]
```

However, it will not reproduce with the following changes.

```
diff -u ../ruby/test.orig.rb ../ruby/test.rb
--- ../ruby/test.orig.rb    2018-01-29 16:41:39.000000000 +0900
+++ ../ruby/test.rb 2018-01-29 16:39:50.000000000 +0900
@@ -9,7 +9,7 @@
       event = parser.pull
       if event.end_element?
         if event[0] == "record"
-          return "foo"
+          puts "foo"
         end
       end
     end
@@ -29,6 +29,6 @@
   event = parser.pull
   # if it's the start of a record element
   if event.start_element? and event[0] == 'record'
-    puts look_at_record(parser)
+    look_at_record(parser)
   end
 end
```

#4 - 01/30/2018 05:32 AM - nobu (Nobuyoshi Nakada)

- Backport changed from 2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: UNKNOWN to 2.3: DONTNEED, 2.4: DONTNEED, 2.5: REQUIRED

- Status changed from Open to Closed

#5 - 02/06/2018 10:29 PM - jrochkind (jonathan rochkind)

Hello, can you explain why this issue closed?

I hope it is seen as a bug? While small changes make it not reproduce, I believe a core dump crash is a bug regardless? Especially when did not that cause that on earlier versions of ruby?

#6 - 02/07/2018 03:00 AM - nagachika (Tomoyuki Chikanaga)

Hello jonathan,

This ticket was marked as duplicated with [Bug #14273] by nobu.
[Bug #14273] was closed by changesets r61617 and r61618.
I hope this issue was fixed in trunk.

nobu also mark this ticket as "REQUIRED to be backported to 2.5 branch".
Stay tuned for the release of 2.5.1.

Regrads,

#7 - 03/24/2018 04:02 PM - naruse (Yui NARUSE)

- Backport changed from 2.3: DONTNEED, 2.4: DONTNEED, 2.5: REQUIRED to 2.3: DONTNEED, 2.4: DONTNEED, 2.5: DONE

ruby_2_5 r62911 merged revision(s) 61587,61617,61618.