Ruby master - Bug #16654
Segfault in rb_str_hash

02/25/2020 07:32 PM - nateberkopec (Nate Berkopec)

Status: Feedback
Priority: Normal
Assignee:
Target version:
ruby -v: ruby 2.6.5p114 (2019-10-01 revision 67812) [x86_64-darwin18]

Backport: 2.5: UNKNOWN, 2.6: UNKNOWN, 2.7: UNKNOWN

Description

Seen in ruby 2.6.5.

-- C level backtrace information ---------------------------------------------
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(rb_vm_bugreport+0x82) [0x10632d9c2]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(rb_bug_context+0x1d8) [0x1061940a8]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(sigsegv+0x51) [0x10629be41]
/usr/lib/system/libsystem_platform.dylib(_sigtramp+0x1d) [0x7fff67bd442d]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(ruby_sip_hash13+0xf0) [0x106257bf0]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(rb_str_hash+0x6c) [0x1062b035c]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(st_general_delete+0x27) [0x1062a5287]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(rb_str_free+0x61) [0x1062b3401]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(obj_free+0x270) [0x1061bbf30]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(gc_sweep_step+0x24c) [0x1061bb56c]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(gc_sweep+0x2db) [0x1061bd37b]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(gc_start+0xa48) [0x1061bfac8]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(gc_start_internal+0x282) [0x1061b7a32]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(vm_call_cfunc+0x15b) [0x1063210fb]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(vm_exec_core+0x33aa) [0x10630b19a]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(rb_vm_exec+0xa0c) [0x10631c04c]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(rb_exec_inter+0x8d8) [0x10619eeb8]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(rb_run_node+0x4a9) [0x10619ed49]
/Users/nateberkopec/.rubies/ruby-2.6.5/bin/ruby(main+0x5d) [0x10611775d]

Another dump posted here:
https://github.com/SamSaffron/memory_profiler/issues/83

For reproduction, I was wrapping MemoryProfiler around a Rails application startup, but it may be possible to repro this in a much simpler way.

```ruby
require "memory_profiler"
report = MemoryProfiler.report do
  require File.expand_path('../config/environment', __FILE__)
end
report.pretty_print
```

History

#1 - 02/25/2020 07:34 PM - nateberkopec (Nate Berkopec)

This reproduces on 2.7.0 as well (though the thing calling rb_str_hash was different, this time objspace_each_objects)

-- C level backtrace information ---------------------------------------------
/Users/nateberkopec/.rubies/ruby-2.7.0/bin/ruby(rb_vm_bugreport+0x96) [0x10089ef76]
/Users/nateberkopec/.rubies/ruby-2.7.0/bin/ruby(rb_bug_for_fatal_signal+0x1d1) [0x1006e5131]
/Users/nateberkopec/.rubies/ruby-2.7.0/bin/ruby(sigsegv+0x5b) [0x100805b4b]
/usr/lib/system/libsystem_platform.dylib(_sigtramp+0x1d) [0x7fff67bd442d]
/Users/nateberkopec/.rubies/ruby-2.7.0/bin/ruby(ruby_sip_hash13+0xf0) [0x10076bdf0]
/Users/nateberkopec/.rubies/ruby-2.7.0/bin/ruby(rb_str_hash+0x6c) [0x100717df]
/Users/nateberkopec/.rubies/ruby-2.7.0/bin/ruby(rb_str_free+0x61) [0x100719f9c]
/Users/nateberkopec/.rubies/ruby-2.7.0/bin/ruby(rb_any_hash+0xfb) [0x10071ddcb]
/Users/nateberkopec/.rubies/ruby-2.7.0/bin/ruby(rb_st_lookup+0x26) [0x10080dcd6]
/Users/nateberkopec/.rubies/ruby-2.7.0/bin/ruby(rb_hash_aref+0x9f) [0x1007171df]
Does not reproduce on 2.5.5, and reproduces on 2.6.0

Unfortunately, doesn't reproduce with a simple script, e.g.:

```ruby
require "memory_profiler"
report = MemoryProfiler.report do
  1_000_000.times { "allocate a string" }
end
report.pretty_print
```

I couldn't reproduce it with a simple file.
Could you try with the master, and could your "config/environment.rb" be shared?

Nobu, This looks like Mac to me maybe llvm related?

The application I'm reproducing it on is here: [https://github.com/codetriage/codetriage](https://github.com/codetriage/codetriage)

I think you should be able to "bundle install" and then use my script above and it would reproduce.

Files

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Date</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>diagnostic_report.crash</td>
<td>44.1 KB</td>
<td>02/25/2020</td>
<td>nateberkopec (Nate Berkopec)</td>
</tr>
<tr>
<td>rubycrashdump.txt</td>
<td>3.47 KB</td>
<td>02/25/2020</td>
<td>nateberkopec (Nate Berkopec)</td>
</tr>
</tbody>
</table>