

Ruby - Bug #19159

ObjectSpace segfaults

11/29/2022 01:10 PM - matsuda (Akira Matsuda)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 3.2.0dev (2022-11-29T09:23:00Z master 67ae3e9738) +YJIT [arm64-darwin21]	Backport: 2.7: UNKNOWN, 3.0: UNKNOWN, 3.1: UNKNOWN

Description

```
$ ruby -e 'p ObjectSpace.each_object.to_a'
```

segfaults on my M1MBP as follows:

```
$ ruby -e 'p ObjectSpace.each_object.to_a'
-e:1: [BUG] Segmentation fault at 0x0000000000000000
ruby 3.2.0dev (2022-11-29T09:23:00Z master 67ae3e9738) +YJIT [arm64-darwin21]
```

```
-- Crash Report log information -----
See Crash Report log file in one of the following locations:
  * ~/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:0005 p:---- s:0017 e:000016 CFUNC :inspect
c:0004 p:---- s:0014 e:000013 CFUNC :inspect
c:0003 p:---- s:0011 e:000010 CFUNC :p
c:0002 p:0009 s:0006 e:000005 EVAL -e:1 [FINISH]
c:0001 p:0000 s:0003 E:0005a0 DUMMY [FINISH]
```

```
-- Ruby level backtrace information -----
-e:1:in `<main>'
-e:1:in `p'
-e:1:in `inspect'
-e:1:in `inspect'
```

```
-- Machine register context -----
x0: 0x0000000000000000 x1: 0x0000000000000004 x2: 0x0000000000000001
x3: 0x00000000104090e94 x4: 0x00000000000000275 x5: 0x00000000000000ad1
x6: 0x00000000000000020 x7: 0x0000000016ef18a00 x18: 0x0000000000000000
x19: 0x00000000000000000 x20: 0x00000000000000001 x21: 0x0000000000000004
x22: 0x00000000104090e98 x23: 0x00000000000000001 x24: 0x0000000000000000
x25: 0x00000000000000001 x26: 0x00000000158127f00 x27: 0x000006000032ab4b0
x28: 0x00000000055550083 lr: 0x0000000010108a058 fp: 0x0000000016ef1a0f0
sp: 0x0000000016ef1a0b0
```

```
-- C level backtrace information -----
~/rbenv/versions/3.2.0-dev/bin/ruby(rb_vm_bugreport+0x2410000000009ac) [0x24100010115a564]
~/rbenv/versions/3.2.0-dev/bin/ruby(rb_bug_for_fatal_signal) [0x9b16000100f7fe68]
~/rbenv/versions/3.2.0-dev/bin/ruby(sig_do_nothing) [0x646c0001010b9638]
/usr/lib/system/libsystem_platform.dylib(_sigtramp+0x664c000000000038) [0x664c0001a77f34a4]
[0x38]
```

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

* Loaded script: -e

* Loaded features:
```

```

0 enumerator.so
1 thread.rb
2 fiber.so
3 rational.so
4 complex.so
5 ruby2_keywords.rb
6 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/arm64-darwin21/enc/encdb.bundle
7 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/arm64-darwin21/enc/trans/transdb.bundle
8 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/arm64-darwin21/rbconfig.rb
9 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/compatibility.rb
10 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/defaults.rb
11 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/deprecate.rb
12 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/errors.rb
13 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/unknown_command_spell_checker.rb
14 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/exceptions.rb
15 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/basic_specification.rb
16 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/stub_specification.rb
17 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/platform.rb
18 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/util/list.rb
19 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/version.rb
20 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/requirement.rb
21 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/specification.rb
22 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/util.rb
23 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/dependency.rb
24 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/core_ext/kernel_gem.rb
25 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/arm64-darwin21/monitor.bundle
26 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/monitor.rb
27 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/core_ext/kernel_require.rb
28 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/core_ext/kernel_warn.rb
29 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems.rb
30 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/path_support.rb
31 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/error_highlight/version.rb
32 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/error_highlight/base.rb
33 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/error_highlight/formatter.rb
34 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/error_highlight/core_ext.rb
35 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/error_highlight.rb
36 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/version.rb
37 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/core_ext/name_error.rb
38 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/levenshtein.rb
39 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/jaro_winkler.rb
40 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checker.rb
41 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checkers/name_error_checkers
/class_name_checker.rb
42 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checkers/name_error_checkers
/variable_name_checker.rb
43 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checkers/name_error_checkers
.rb
44 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checkers/method_name_checker
.rb
45 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checkers/key_error_checker.r
b
46 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checkers/null_checker.rb
47 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/tree_spell_checker.rb
48 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checkers/require_path_checke
r.rb
49 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checkers/pattern_key_name_ch
ecker.rb
50 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/formatter.rb
51 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean.rb
52 ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/syntax_suggest/core_ext.rb

```

* Process memory map:

```

100ee4000-101390000 r-x ~/.rbenv/versions/3.2.0-dev/bin/ruby
101390000-1013ac000 r-- ~/.rbenv/versions/3.2.0-dev/bin/ruby
1013ac000-1013b0000 rw- ~/.rbenv/versions/3.2.0-dev/bin/ruby

```

```

1013b0000-1013c0000 rw- ~/.rbenv/versions/3.2.0-dev/bin/ruby
1013c0000-1015a8000 r-- ~/.rbenv/versions/3.2.0-dev/bin/ruby
1015a8000-1016a8000 r-- /usr/lib/dyld
1016a8000-1016b0000 rw- /usr/lib/dyld
1016b0000-1016b4000 r-- /usr/lib/dyld
1016b4000-1016b8000 r-- /usr/lib/dyld
1016b8000-1016bc000 rw- /usr/lib/dyld
1016bc000-1016c0000 --- /usr/lib/dyld
1016c0000-1016c8000 rw- /usr/lib/dyld
1016c8000-1016cc000 --- /usr/lib/dyld
1016cc000-1016d0000 --- /usr/lib/dyld
1016d0000-1016d8000 rw- /usr/lib/dyld
1016d8000-1016dc000 --- /usr/lib/dyld
1016dc000-1016e0000 --- /usr/lib/dyld
1016e0000-1016e8000 rw- /usr/lib/dyld
1016e8000-1016ec000 --- /usr/lib/dyld
1016ec000-1016f0000 r-- /usr/lib/dyld
1016f0000-1016f4000 r-- /usr/lib/dyld
1016f4000-1016f8000 rw- /usr/lib/dyld
1016f8000-1016fc000 r-- /usr/lib/dyld
1016fc000-10173c000 rw- /usr/lib/dyld
101740000-101750000 rw- /usr/lib/dyld
10175c000-1017bc000 r-x /usr/lib/dyld
1017bc000-1017d4000 r-- /usr/lib/dyld
1017d4000-1017d8000 rw- /usr/lib/dyld
1017d8000-101810000 r-- /usr/lib/dyld
101810000-101868000 r-x /opt/homebrew/Cellar/gmp/6.2.1_1/lib/libgmp.10.dylib
101868000-10186c000 r-- /opt/homebrew/Cellar/gmp/6.2.1_1/lib/libgmp.10.dylib
10186c000-101870000 rw- /opt/homebrew/Cellar/gmp/6.2.1_1/lib/libgmp.10.dylib
101870000-101880000 r-- /opt/homebrew/Cellar/gmp/6.2.1_1/lib/libgmp.10.dylib
101880000-101884000 r-x ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/arm64-darwin21/enc/encdb.bundle
101884000-101888000 r-- ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/arm64-darwin21/enc/encdb.bundle
101888000-10188c000 r-- ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/arm64-darwin21/enc/encdb.bundle
101890000-1018a0000 rw- ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/arm64-darwin21/enc/trans/transdb.bundle
1018a0000-1018a4000 r-x ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/arm64-darwin21/enc/trans/transdb.bundle
1018a4000-1018a8000 r-- ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/arm64-darwin21/enc/trans/transdb.bundle
1018a8000-1018ac000 r-- ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/arm64-darwin21/enc/trans/transdb.bundle
1018b0000-1018c0000 rw- ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/arm64-darwin21/monitor.bundle
1018c0000-1018c4000 r-x ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/arm64-darwin21/monitor.bundle
1018c4000-1018c8000 r-- ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/arm64-darwin21/monitor.bundle
1018c8000-1018cc000 rw- ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/arm64-darwin21/monitor.bundle
1018cc000-1018d0000 r-- ~/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/arm64-darwin21/monitor.bundle
1018d0000-1018e0000 rw- ~/.rbenv/versions/3.2.0-dev/bin/ruby
1018f0000-101900000 rw- ~/.rbenv/versions/3.2.0-dev/bin/ruby
101910000-101920000 rw- ~/.rbenv/versions/3.2.0-dev/bin/ruby
101920000-102920000 rw- ~/.rbenv/versions/3.2.0-dev/bin/ruby
102930000-102940000 rw- ~/.rbenv/versions/3.2.0-dev/bin/ruby
102950000-102960000 rw- ~/.rbenv/versions/3.2.0-dev/bin/ruby
102970000-102980000 rw- ~/.rbenv/versions/3.2.0-dev/bin/ruby
102980000-102984000 --- ~/.rbenv/versions/3.2.0-dev/bin/ruby
102984000-102a28000 rw- ~/.rbenv/versions/3.2.0-dev/bin/ruby
102a28000-102a2c000 --- ~/.rbenv/versions/3.2.0-dev/bin/ruby
102a2c000-102ad0000 rw- ~/.rbenv/versions/3.2.0-dev/bin/ruby
102ad0000-102ad4000 --- ~/.rbenv/versions/3.2.0-dev/bin/ruby
102ad4000-102b78000 rw- ~/.rbenv/versions/3.2.0-dev/bin/ruby
102b78000-102b7c000 --- ~/.rbenv/versions/3.2.0-dev/bin/ruby
102b7c000-102c20000 rw- ~/.rbenv/versions/3.2.0-dev/bin/ruby
102c20000-102c24000 --- ~/.rbenv/versions/3.2.0-dev/bin/ruby
102c24000-102cc8000 rw- ~/.rbenv/versions/3.2.0-dev/bin/ruby
102cc8000-102ccc000 --- ~/.rbenv/versions/3.2.0-dev/bin/ruby

```

102ccc000-102d70000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
102d70000-102d74000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
102d74000-102e18000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
102e18000-102e1c000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
102e1c000-102ec0000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
102ec0000-102ec4000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
102ec4000-102f68000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
102f68000-102f6c000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
102f6c000-103010000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103010000-103014000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
103014000-1030b8000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
1030b8000-1030bc000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
1030bc000-103160000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103160000-103164000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
103164000-103208000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103208000-10320c000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
10320c000-1032b0000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
1032b0000-1032b4000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
1032b4000-103358000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103358000-10335c000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
10335c000-103400000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103400000-103404000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
103404000-1034a8000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
1034a8000-1034ac000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
1034ac000-103550000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103550000-103554000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
103554000-1035f8000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
1035f8000-1035fc000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
1035fc000-1036a0000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
1036a0000-1036a4000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
1036a4000-103748000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103748000-10374c000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
10374c000-1037f0000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
1037f0000-1037f4000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
1037f4000-103898000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103898000-10389c000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
10389c000-103940000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103940000-103944000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
103944000-1039e8000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
1039e8000-1039ec000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
1039ec000-103a90000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103a90000-103a94000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
103a94000-103b38000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103b38000-103b3c000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
103b3c000-103be0000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103be0000-103be4000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
103be4000-103c88000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103c88000-103c8c000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
103c8c000-103d30000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103d30000-103d34000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
103d34000-103dd8000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103dd8000-103ddc000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
103ddc000-103e80000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103e80000-103ea0000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103eb0000-103ec0000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103ed0000-103ee0000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103ef0000-103f00000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103f10000-103f20000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103f30000-103f40000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103f50000-103f60000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103f70000-103f80000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103f90000-103fa0000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103fb0000-103fc0000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103fd0000-103fe0000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
103ff0000-104000000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
104010000-104020000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
104030000-104040000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby

104050000-104060000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
104070000-104080000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
104090000-1040a0000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
1040b0000-1040c0000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
1040d0000-1040e0000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
1040e0000-1040e4000	r-x	~/rbenv/versions/3.2.0-dev/bin/ruby
1040e4000-1040e8000	r-x	~/rbenv/versions/3.2.0-dev/bin/ruby
1040e8000-10c0e0000	---	~/rbenv/versions/3.2.0-dev/bin/ruby
10c0f0000-10c100000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
10c110000-10c120000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
10c130000-10c140000	rw-	~/rbenv/versions/3.2.0-dev/bin/ruby
10c140000-10c7f4000	r--	~/rbenv/versions/3.2.0-dev/bin/ruby
10c7f4000-10cea8000	r--	~/rbenv/versions/3.2.0-dev/bin/ruby
138000000-138800000	rw-	
138800000-139000000	rw-	
139000000-139800000	rw-	
139800000-13a000000	rw-	
13a000000-13a800000	rw-	
13a800000-13b000000	rw-	
13b000000-13b800000	rw-	
13b800000-13c000000	rw-	
13c000000-13c800000	rw-	
13c800000-13d000000	rw-	
13d000000-13d800000	rw-	
13d800000-13e000000	rw-	
13e000000-13e800000	rw-	
13e800000-13f000000	rw-	
13f000000-13f800000	rw-	
13f800000-140000000	rw-	
146e00000-146f00000	rw-	
146f00000-147000000	rw-	
147000000-147800000	rw-	
147800000-148000000	rw-	
148000000-148800000	rw-	
148800000-149000000	rw-	
149000000-149800000	rw-	
149800000-14a000000	rw-	
14a000000-14a800000	rw-	
14a800000-14b000000	rw-	
14b000000-14b800000	rw-	
14b800000-14c000000	rw-	
14c000000-14c800000	rw-	
14c800000-14d000000	rw-	
14d000000-14d800000	rw-	
14d800000-14e000000	rw-	
14e000000-14e800000	rw-	
14e800000-14f000000	rw-	
14f000000-14f800000	rw-	
14f800000-150000000	rw-	
156e00000-156f00000	rw-	
156f00000-157000000	rw-	
157000000-157800000	rw-	
157800000-157804000	rw-	
158000000-158800000	rw-	
158800000-159000000	rw-	
159000000-159800000	rw-	
159800000-15a000000	rw-	
15a000000-15a800000	rw-	
15a800000-15b000000	rw-	
15b000000-15b800000	rw-	
15b800000-15c000000	rw-	
15c000000-15c800000	rw-	
15c800000-15d000000	rw-	
15d000000-15d800000	rw-	
15d800000-15e000000	rw-	
15e000000-15e800000	rw-	
15e800000-15f000000	rw-	

```
15f000000-15f800000 rw-
15f800000-160000000 rw-
160000000-162000000 rw-
162000000-162800000 rw-
16af1c000-16e720000 ---
16e720000-16ef1c000 rw-
16ef1c000-16ef20000 ---
16ef20000-16efa8000 rw-
180000000-1fc000000 r--
1fc000000-1fd9d8000 r--
1fd9d8000-1fd9fc000 rw-
1fd9fc000-1fe000000 rw-
1fe000000-200000000 r--
200000000-2001e8000 r--
2001e8000-2018dc000 rw-
2018dc000-204c64000 r--
204c64000-206000000 r--
206000000-236000000 r--
236000000-236a10000 r--
236a10000-2377f4000 rw-
2377f4000-238ac0000 r--
238ac0000-23a000000 r--
23a000000-280000000 r--
fc0000000-1000000000 ---
1000000000-7000000000 ---
600000000000-600008000000 rw-
600008000000-600010000000 rw-
600010000000-600018000000 rw-
600018000000-600020000000 rw-
[IMPORTANT]
Don't forget to include the Crash Report log file under
DiagnosticReports directory in bug reports.
```

Related issues:

Related to Ruby - Bug #19156: ObjectSpace.dump_all segfault during string ins...

Third Party's Issue

Associated revisions

Revision ab4c7077cc44cd6725625562b7380a44cf462190 - 11/30/2022 05:38 PM - mame (Yusuke Endoh)

Prevent segfault in String#scan with ObjectSpace.each_object

Calling String#scan without a block creates an incomplete MatchData object whose RMATCH(match)->str is Qfalse. Usually this object is not leaked, but it was possible to pull it by using ObjectSpace.each_object.

This change hides the internal MatchData object by using rb_obj_hide.

Fixes [Bug #19159]

Revision ab4c7077cc44cd6725625562b7380a44cf462190 - 11/30/2022 05:38 PM - mame (Yusuke Endoh)

Prevent segfault in String#scan with ObjectSpace.each_object

Calling String#scan without a block creates an incomplete MatchData object whose RMATCH(match)->str is Qfalse. Usually this object is not leaked, but it was possible to pull it by using ObjectSpace.each_object.

This change hides the internal MatchData object by using rb_obj_hide.

Fixes [Bug #19159]

Revision ab4c7077 - 11/30/2022 05:38 PM - mame (Yusuke Endoh)

Prevent segfault in String#scan with ObjectSpace.each_object

Calling String#scan without a block creates an incomplete MatchData object whose RMATCH(match)->str is Qfalse. Usually this object is not leaked, but it was possible to pull it by using ObjectSpace.each_object.

This change hides the internal MatchData object by using rb_obj_hide.

History

#1 - 11/30/2022 04:53 AM - hsbt (Hiroshi SHIBATA)

I could reproduce this. And It resolve with --disable-error_highlight. (Thanks for investigating @yahonda)

#2 - 11/30/2022 04:56 AM - hsbt (Hiroshi SHIBATA)

- Related to Bug #19156: ObjectSpace.dump_all segfault during string inspection added

#3 - 11/30/2022 05:06 AM - yahonda (Yasuo Honda)

--disable-error_highlight did not help when I execute it with Ruby 3.2.0dev.

```
$ rbenv install 3.2.0-dev
$ rbenv global 3.2.0-dev
$ ruby -v
ruby 3.2.0dev (2022-11-30T04:52:33Z master 9a84971315) [x86_64-linux]

$ ruby -e 'p ObjectSpace.each_object.to_a' --disable-error_highlight
-e:1: [BUG] Segmentation fault at 0x0000000000000010
ruby 3.2.0dev (2022-11-30T04:52:33Z master 9a84971315) [x86_64-linux]

-- Control frame information -----
c:0005 p:---- s:0017 e:000016 CFUNC :inspect
c:0004 p:---- s:0014 e:000013 CFUNC :inspect
c:0003 p:---- s:0011 e:000010 CFUNC :p
c:0002 p:0009 s:0006 e:000005 EVAL -e:1 [FINISH]
c:0001 p:0000 s:0003 E:001910 DUMMY [FINISH]

-- Ruby level backtrace information -----
-e:1:in `<main>'
-e:1:in `p'
-e:1:in `inspect'
-e:1:in `inspect'

-- Machine register context -----
RIP: 0x000056335bed3a5c RBP: 0x0000000000000001 RSP: 0x00007ffcb5848780
RAX: 0x0000000000000005 RBX: 0x0000000000000000 RCX: 0x0000000000000020
RDX: 0x0000000000000001 RDI: 0x0000000000000000 RSI: 0x0000000000000004
R8: 0x00007fd6c4679410 R9: 0x00007fd6c9e6c600 R10: 0xffffffffffffffff
R11: 0x00007fd6c4689fc8 R12: 0x0000000000000004 R13: 0x00007fd6c46793f8
R14: 0x00007ffcb58487f0 R15: 0x0000000000000000 EFL: 0x0000000000010246

-- C level backtrace information -----
ruby(rb_vm_bugreport+0x5cf) [0x56335bf7237f]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(rb_bug_for_fatal_signal+0xec) [0x56335c01ca2c]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(sigsegv+0x4f) [0x56335bebc92f]
[0x7fd6c9c3bcf0]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(str_subseq+0x2c) [0x56335bed3a5c]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(rb_str_subseq+0x12) [0x56335bee2df2]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(match_inspect+0x18c) [0x56335be88acc]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(vm_call0_body+0x135) [0x56335bf5ba95]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(rb_funcallv_scope+0x1b1) [0x56335bf5fb11]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(rb_inspect+0x18) [0x56335be130b8]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(inspect_ary+0x61) [0x56335bf7fa11]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(exec_recursive+0x446) [0x56335bef696]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(vm_call0_body+0x135) [0x56335bf5ba95]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(rb_funcallv_scope+0x1b1) [0x56335bf5fb11]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(rb_inspect+0x18) [0x56335be130b8]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(rb_f_p+0x44) [0x56335bd9e7d4]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(vm_call_cfunc_with_frame+0x11f) [0x56335bf47a9f]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(vm_exec_core+0x10b) [0x56335bf643cb]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(rb_vm_exec+0x177) [0x56335bf54a17]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(rb_ec_exec_node+0xb1) [0x56335bd581a1]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(ruby_run_node+0x4c) [0x56335bd5d43c]
/home/yahonda/.rbenv/versions/3.2.0-dev/bin/ruby(main+0x66) [0x56335bd57e16]

-- Other runtime information -----

* Loaded script: -e

* Loaded features:
```

```

0 enumerator.so
1 thread.rb
2 fiber.so
3 rational.so
4 complex.so
5 ruby2_keywords.rb
6 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/x86_64-linux/enc/encdb.so
7 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/x86_64-linux/enc/trans/transdb.so
8 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/x86_64-linux/rbconfig.rb
9 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/compatibility.rb
10 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/defaults.rb
11 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/deprecate.rb
12 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/errors.rb
13 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/unknown_command_spell_checker.rb
14 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/exceptions.rb
15 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/basic_specification.rb
16 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/stub_specification.rb
17 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/platform.rb
18 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/util/list.rb
19 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/version.rb
20 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/requirement.rb
21 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/specification.rb
22 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/util.rb
23 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/dependency.rb
24 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/core_ext/kernel_gem.rb
25 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/x86_64-linux/monitor.so
26 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/monitor.rb
27 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/core_ext/kernel_require.rb
28 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/core_ext/kernel_warn.rb
29 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems.rb
30 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/rubygems/path_support.rb
31 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/version.rb
32 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/core_ext/name_error.rb
33 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/levenshtein.rb
34 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/jaro_winkler.rb
35 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checker.rb
36 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checkers/name_error_checkers
/class_name_checker.rb
37 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checkers/name_error_checkers
/variable_name_checker.rb
38 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checkers/name_error_checkers
.rb
39 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checkers/method_name_checker
.rb
40 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checkers/key_error_checker.r
b
41 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checkers/null_checker.rb
42 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/tree_spell_checker.rb
43 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checkers/require_path_checke
r.rb
44 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/spell_checkers/pattern_key_name_ch
ecker.rb
45 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean/formatter.rb
46 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/did_you_mean.rb
47 /home/yahonda/.rbenv/versions/3.2.0-dev/lib/ruby/3.2.0+3/syntax_suggest/core_ext.rb

```

* Process memory map:

```

56335bd24000-56335bd53000 r--p 00000000 103:02 24117809 /home/yahonda/.rbenv/versions/3.2.0-d
ev/bin/ruby
56335bd53000-56335c029000 r-xp 0002f000 103:02 24117809 /home/yahonda/.rbenv/versions/3.2.0-d
ev/bin/ruby
56335c029000-56335c160000 r--p 00305000 103:02 24117809 /home/yahonda/.rbenv/versions/3.2.0-d
ev/bin/ruby
56335c160000-56335c16a000 r--p 0043b000 103:02 24117809 /home/yahonda/.rbenv/versions/3.2.0-d
ev/bin/ruby
56335c16a000-56335c16b000 rw-p 00445000 103:02 24117809 /home/yahonda/.rbenv/versions/3.2.0-d
ev/bin/ruby
56335c16b000-56335c17c000 rw-p 00000000 00:00 0
56335c335000-56335c846000 rw-p 00000000 00:00 0 [heap]
7fd6c1400000-7fd6c2dda000 r--s 00000000 103:02 24117809 /home/yahonda/.rbenv/versions/3.2.0-d
ev/bin/ruby
7fd6c2e3a000-7fd6c363b000 rw-p 00000000 00:00 0
7fd6c363b000-7fd6c3e3c000 rw-p 00000000 00:00 0
7fd6c457f000-7fd6c45d0000 rw-p 00000000 00:00 0

```


7fd6c45f0000-7fd6c45f3000	r--p	00000000	103:02	42998345	/usr/lib/x86_64-linux-gnu/libgcc_s.so.1
7fd6c45f3000-7fd6c460a000	r-xp	00003000	103:02	42998345	/usr/lib/x86_64-linux-gnu/libgcc_s.so.1
7fd6c460a000-7fd6c460e000	r--p	0001a000	103:02	42998345	/usr/lib/x86_64-linux-gnu/libgcc_s.so.1
7fd6c460e000-7fd6c460f000	r--p	0001d000	103:02	42998345	/usr/lib/x86_64-linux-gnu/libgcc_s.so.1
7fd6c460f000-7fd6c4610000	rw-p	0001e000	103:02	42998345	/usr/lib/x86_64-linux-gnu/libgcc_s.so.1
7fd6c4610000-7fd6c4750000	rw-p	00000000	00:00	0	
7fd6c4756000-7fd6c4757000	---p	00000000	00:00	0	
7fd6c4757000-7fd6c47f8000	rw-p	00000000	00:00	0	
7fd6c47f8000-7fd6c47f9000	---p	00000000	00:00	0	
7fd6c47f9000-7fd6c489a000	rw-p	00000000	00:00	0	
7fd6c489a000-7fd6c489b000	---p	00000000	00:00	0	
7fd6c489b000-7fd6c493c000	rw-p	00000000	00:00	0	
7fd6c493c000-7fd6c493d000	---p	00000000	00:00	0	
7fd6c493d000-7fd6c49de000	rw-p	00000000	00:00	0	
7fd6c49de000-7fd6c49df000	---p	00000000	00:00	0	
7fd6c49df000-7fd6c4a80000	rw-p	00000000	00:00	0	
7fd6c4a80000-7fd6c4a81000	---p	00000000	00:00	0	
7fd6c4a81000-7fd6c4b22000	rw-p	00000000	00:00	0	
7fd6c4b22000-7fd6c4b23000	---p	00000000	00:00	0	
7fd6c4b23000-7fd6c4bc4000	rw-p	00000000	00:00	0	
7fd6c4bc4000-7fd6c4bc5000	---p	00000000	00:00	0	
7fd6c4bc5000-7fd6c4c66000	rw-p	00000000	00:00	0	
7fd6c4c66000-7fd6c4c67000	---p	00000000	00:00	0	
7fd6c4c67000-7fd6c4d08000	rw-p	00000000	00:00	0	
7fd6c4d08000-7fd6c4d09000	---p	00000000	00:00	0	
7fd6c4d09000-7fd6c4daa000	rw-p	00000000	00:00	0	
7fd6c4daa000-7fd6c4dab000	---p	00000000	00:00	0	
7fd6c4dab000-7fd6c4e4c000	rw-p	00000000	00:00	0	
7fd6c4e4c000-7fd6c4e4d000	---p	00000000	00:00	0	
7fd6c4e4d000-7fd6c4eee000	rw-p	00000000	00:00	0	
7fd6c4eee000-7fd6c4eef000	---p	00000000	00:00	0	
7fd6c4eef000-7fd6c4f90000	rw-p	00000000	00:00	0	
7fd6c4f90000-7fd6c4f91000	---p	00000000	00:00	0	
7fd6c4f91000-7fd6c5032000	rw-p	00000000	00:00	0	
7fd6c5032000-7fd6c5033000	---p	00000000	00:00	0	
7fd6c5033000-7fd6c50d4000	rw-p	00000000	00:00	0	
7fd6c50d4000-7fd6c50d5000	---p	00000000	00:00	0	
7fd6c50d5000-7fd6c5176000	rw-p	00000000	00:00	0	
7fd6c5176000-7fd6c5177000	---p	00000000	00:00	0	
7fd6c5177000-7fd6c5218000	rw-p	00000000	00:00	0	
7fd6c5218000-7fd6c5219000	---p	00000000	00:00	0	
7fd6c5219000-7fd6c52ba000	rw-p	00000000	00:00	0	
7fd6c52ba000-7fd6c52bb000	---p	00000000	00:00	0	
7fd6c52bb000-7fd6c535c000	rw-p	00000000	00:00	0	
7fd6c535c000-7fd6c535d000	---p	00000000	00:00	0	
7fd6c535d000-7fd6c53fe000	rw-p	00000000	00:00	0	
7fd6c53fe000-7fd6c53ff000	---p	00000000	00:00	0	
7fd6c53ff000-7fd6c54a0000	rw-p	00000000	00:00	0	
7fd6c54a0000-7fd6c54a1000	---p	00000000	00:00	0	
7fd6c54a1000-7fd6c5542000	rw-p	00000000	00:00	0	
7fd6c5542000-7fd6c5543000	---p	00000000	00:00	0	
7fd6c5543000-7fd6c55e4000	rw-p	00000000	00:00	0	
7fd6c55e4000-7fd6c55e5000	---p	00000000	00:00	0	
7fd6c55e5000-7fd6c5686000	rw-p	00000000	00:00	0	
7fd6c5686000-7fd6c5687000	---p	00000000	00:00	0	
7fd6c5687000-7fd6c5728000	rw-p	00000000	00:00	0	
7fd6c5728000-7fd6c5729000	---p	00000000	00:00	0	
7fd6c5729000-7fd6c57ca000	rw-p	00000000	00:00	0	
7fd6c57ca000-7fd6c57cb000	---p	00000000	00:00	0	
7fd6c57cb000-7fd6c586c000	rw-p	00000000	00:00	0	
7fd6c586c000-7fd6c586d000	---p	00000000	00:00	0	
7fd6c586d000-7fd6c590e000	rw-p	00000000	00:00	0	
7fd6c590e000-7fd6c590f000	---p	00000000	00:00	0	
7fd6c590f000-7fd6c59b0000	rw-p	00000000	00:00	0	
7fd6c59b0000-7fd6c59b1000	---p	00000000	00:00	0	
7fd6c59b1000-7fd6c5a52000	rw-p	00000000	00:00	0	
7fd6c5a52000-7fd6c5a53000	---p	00000000	00:00	0	
7fd6c5a53000-7fd6c5af4000	rw-p	00000000	00:00	0	
7fd6c5af4000-7fd6c5af5000	---p	00000000	00:00	0	
7fd6c5af5000-7fd6c8c00000	rw-p	00000000	00:00	0	

7fd6c8c00000-7fd6c9aed000	r--p	00000000	103:02	42997062	/usr/lib/locale/locale-archive
7fd6c9aff000-7fd6c9c00000	rw-p	00000000	00:00	0	
7fd6c9c00000-7fd6c9c22000	r--p	00000000	103:02	42998042	/usr/lib/x86_64-linux-gnu/libc.so.6
7fd6c9c22000-7fd6c9d9b000	r-xp	00022000	103:02	42998042	/usr/lib/x86_64-linux-gnu/libc.so.6
7fd6c9d9b000-7fd6c9df2000	r--p	0019b000	103:02	42998042	/usr/lib/x86_64-linux-gnu/libc.so.6
7fd6c9df2000-7fd6c9df6000	r--p	001f1000	103:02	42998042	/usr/lib/x86_64-linux-gnu/libc.so.6
7fd6c9df6000-7fd6c9df8000	rw-p	001f5000	103:02	42998042	/usr/lib/x86_64-linux-gnu/libc.so.6
7fd6c9df8000-7fd6c9e05000	rw-p	00000000	00:00	0	
7fd6c9e20000-7fd6c9eb0000	rw-p	00000000	00:00	0	
7fd6c9eb9000-7fd6c9eba000	r--p	00000000	103:02	24117815	/home/yahonda/.rbenv/versions/3.2.0-d
ev/lib/ruby/3.2.0+3/x86_64-linux/monitor.so					
7fd6c9eba000-7fd6c9ebb000	r-xp	00001000	103:02	24117815	/home/yahonda/.rbenv/versions/3.2.0-d
ev/lib/ruby/3.2.0+3/x86_64-linux/monitor.so					
7fd6c9ebb000-7fd6c9ebc000	r--p	00002000	103:02	24117815	/home/yahonda/.rbenv/versions/3.2.0-d
ev/lib/ruby/3.2.0+3/x86_64-linux/monitor.so					
7fd6c9ebc000-7fd6c9ebd000	r--p	00002000	103:02	24117815	/home/yahonda/.rbenv/versions/3.2.0-d
ev/lib/ruby/3.2.0+3/x86_64-linux/monitor.so					
7fd6c9ebd000-7fd6c9ebe000	rw-p	00003000	103:02	24117815	/home/yahonda/.rbenv/versions/3.2.0-d
ev/lib/ruby/3.2.0+3/x86_64-linux/monitor.so					
7fd6c9ebe000-7fd6c9f15000	r--p	00000000	103:02	43127753	/usr/lib/locale/C.utf8/LC_CTYPE
7fd6c9f15000-7fd6c9f1a000	rw-p	00000000	00:00	0	
7fd6c9f1a000-7fd6c9f28000	r--p	00000000	103:02	42998712	/usr/lib/x86_64-linux-gnu/libm.so.6
7fd6c9f28000-7fd6c9fa6000	r-xp	0000e000	103:02	42998712	/usr/lib/x86_64-linux-gnu/libm.so.6
7fd6c9fa6000-7fd6ca001000	r--p	0008c000	103:02	42998712	/usr/lib/x86_64-linux-gnu/libm.so.6
7fd6ca001000-7fd6ca002000	r--p	000e6000	103:02	42998712	/usr/lib/x86_64-linux-gnu/libm.so.6
7fd6ca002000-7fd6ca003000	rw-p	000e7000	103:02	42998712	/usr/lib/x86_64-linux-gnu/libm.so.6
7fd6ca003000-7fd6ca005000	r--p	00000000	103:02	42998122	/usr/lib/x86_64-linux-gnu/libcrypt.so
.1.1.0					
7fd6ca005000-7fd6ca019000	r-xp	00002000	103:02	42998122	/usr/lib/x86_64-linux-gnu/libcrypt.so
.1.1.0					
7fd6ca019000-7fd6ca032000	r--p	00016000	103:02	42998122	/usr/lib/x86_64-linux-gnu/libcrypt.so
.1.1.0					
7fd6ca032000-7fd6ca033000	r--p	0002f000	103:02	42998122	/usr/lib/x86_64-linux-gnu/libcrypt.so
.1.1.0					
7fd6ca033000-7fd6ca034000	rw-p	00030000	103:02	42998122	/usr/lib/x86_64-linux-gnu/libcrypt.so
.1.1.0					
7fd6ca034000-7fd6ca03c000	rw-p	00000000	00:00	0	
7fd6ca03c000-7fd6ca046000	r--p	00000000	103:02	42998406	/usr/lib/x86_64-linux-gnu/libgmp.so.1
0.4.1					
7fd6ca046000-7fd6ca0a6000	r-xp	0000a000	103:02	42998406	/usr/lib/x86_64-linux-gnu/libgmp.so.1
0.4.1					
7fd6ca0a6000-7fd6ca0bd000	r--p	0006a000	103:02	42998406	/usr/lib/x86_64-linux-gnu/libgmp.so.1
0.4.1					
7fd6ca0bd000-7fd6ca0be000	r--p	00080000	103:02	42998406	/usr/lib/x86_64-linux-gnu/libgmp.so.1
0.4.1					
7fd6ca0be000-7fd6ca0bf000	rw-p	00081000	103:02	42998406	/usr/lib/x86_64-linux-gnu/libgmp.so.1
0.4.1					
7fd6ca0bf000-7fd6ca0c1000	r--p	00000000	103:02	42999435	/usr/lib/x86_64-linux-gnu/libz.so.1.2
.11					
7fd6ca0c1000-7fd6ca0d3000	r-xp	00002000	103:02	42999435	/usr/lib/x86_64-linux-gnu/libz.so.1.2
.11					
7fd6ca0d3000-7fd6ca0d9000	r--p	00014000	103:02	42999435	/usr/lib/x86_64-linux-gnu/libz.so.1.2
.11					
7fd6ca0d9000-7fd6ca0da000	r--p	0001a000	103:02	42999435	/usr/lib/x86_64-linux-gnu/libz.so.1.2
.11					
7fd6ca0da000-7fd6ca0db000	rw-p	0001b000	103:02	42999435	/usr/lib/x86_64-linux-gnu/libz.so.1.2
.11					
7fd6ca0dc000-7fd6ca0dd000	r--p	00000000	103:02	24122073	/home/yahonda/.rbenv/versions/3.2.0-d
ev/lib/ruby/3.2.0+3/x86_64-linux/enc/trans/transdb.so					
7fd6ca0dd000-7fd6ca0de000	r-xp	00001000	103:02	24122073	/home/yahonda/.rbenv/versions/3.2.0-d
ev/lib/ruby/3.2.0+3/x86_64-linux/enc/trans/transdb.so					
7fd6ca0de000-7fd6ca0df000	r--p	00002000	103:02	24122073	/home/yahonda/.rbenv/versions/3.2.0-d
ev/lib/ruby/3.2.0+3/x86_64-linux/enc/trans/transdb.so					
7fd6ca0df000-7fd6ca0e0000	r--p	00002000	103:02	24122073	/home/yahonda/.rbenv/versions/3.2.0-d
ev/lib/ruby/3.2.0+3/x86_64-linux/enc/trans/transdb.so					
7fd6ca0e0000-7fd6ca0e1000	rw-p	00003000	103:02	24122073	/home/yahonda/.rbenv/versions/3.2.0-d
ev/lib/ruby/3.2.0+3/x86_64-linux/enc/trans/transdb.so					
7fd6ca0e1000-7fd6ca0e2000	r--p	00000000	103:02	24117834	/home/yahonda/.rbenv/versions/3.2.0-d
ev/lib/ruby/3.2.0+3/x86_64-linux/enc/encdb.so					
7fd6ca0e2000-7fd6ca0e3000	r-xp	00001000	103:02	24117834	/home/yahonda/.rbenv/versions/3.2.0-d
ev/lib/ruby/3.2.0+3/x86_64-linux/enc/encdb.so					
7fd6ca0e3000-7fd6ca0e4000	r--p	00002000	103:02	24117834	/home/yahonda/.rbenv/versions/3.2.0-d
ev/lib/ruby/3.2.0+3/x86_64-linux/enc/encdb.so					
7fd6ca0e4000-7fd6ca0e5000	r--p	00002000	103:02	24117834	/home/yahonda/.rbenv/versions/3.2.0-d
ev/lib/ruby/3.2.0+3/x86_64-linux/enc/encdb.so					

```

7fd6ca0e5000-7fd6ca0e6000 rw-p 00003000 103:02 24117834 /home/yahonda/.rbenv/versions/3.2.0-d
ev/lib/ruby/3.2.0+3/x86_64-linux/enc/encdb.so
7fd6ca0e6000-7fd6ca0ed000 r--s 00000000 103:02 43651195 /usr/lib/x86_64-linux-gnu/gconv/gconv
-modules.cache
7fd6ca0ed000-7fd6ca0ef000 rw-p 00000000 00:00 0
7fd6ca0ef000-7fd6ca0f0000 r--p 00000000 103:02 42997696 /usr/lib/x86_64-linux-gnu/ld-linux-x8
6-64.so.2
7fd6ca0f0000-7fd6ca119000 r-xp 00001000 103:02 42997696 /usr/lib/x86_64-linux-gnu/ld-linux-x8
6-64.so.2
7fd6ca119000-7fd6ca123000 r--p 0002a000 103:02 42997696 /usr/lib/x86_64-linux-gnu/ld-linux-x8
6-64.so.2
7fd6ca123000-7fd6ca125000 r--p 00034000 103:02 42997696 /usr/lib/x86_64-linux-gnu/ld-linux-x8
6-64.so.2
7fd6ca125000-7fd6ca127000 rw-p 00036000 103:02 42997696 /usr/lib/x86_64-linux-gnu/ld-linux-x8
6-64.so.2
7ffc504d000-7ffc584c000 rw-p 00000000 00:00 0 [stack]
7ffc5883000-7ffc5887000 r--p 00000000 00:00 0 [vvar]
7ffc5887000-7ffc5889000 r-xp 00000000 00:00 0 [vdso]
fffffffff600000-fffffffff601000 --xp 00000000 00:00 0 [vsyscall]

```

Aborted (core dumped)
\$

#4 - 11/30/2022 04:36 PM - mame (Yusuke Endoh)

<https://github.com/ruby/ruby/pull/6836>

An incomplete MatchData object was created during String#scan (which is called for Gem::Version, not error_highlight :-).

#5 - 11/30/2022 07:09 PM - mame (Yusuke Endoh)

- Status changed from Open to Closed

Applied in changeset [gitlab4c7077cc44cd6725625562b7380a44cf462190](https://github.com/ruby/ruby/pull/6836).

Prevent segfault in String#scan with ObjectSpace.each_object

Calling String#scan without a block creates an incomplete MatchData object whose RMATCH(match)->str is Qfalse. Usually this object is not leaked, but it was possible to pull it by using ObjectSpace.each_object.

This change hides the internal MatchData object by using rb_obj_hide.

Fixes [Bug [#19159](#)]

#6 - 11/30/2022 10:40 PM - hsbt (Hiroshi SHIBATA)

I confirmed to work with <https://github.com/ruby/ruby/pull/6836>

#7 - 11/30/2022 11:47 PM - matsuda (Akira Matsuda)

Just confirmed the fix. Thank you for the quick fix, [@mame \(Yusuke Endoh\)](#) !