

Ruby - Bug #19992

Seemingly GC causes double free for regparse

11/07/2023 02:41 PM - mtasaka (Mamoru TASAKA)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 3.3.0dev (2023-11-07 master ced84beb25) [x86_64-linux]	Backport: 3.0: UNKNOWN, 3.1: UNKNOWN, 3.2: UNKNOWN

Description

Using ruby3.3.0dev (now I've tried [ced84beb2518d173988bb92c6d96aa854a35abe6](https://github.com/sporkmonger/addressable/releases/tag/addressable-2.8.5)), trying to execute rubygem-addressable 2.8.5 (<https://github.com/sporkmonger/addressable/releases/tag/addressable-2.8.5>) testsuite causes ruby segfault:

```
$ LC_ALL=C.UTF-8 rspec -I. spec/
Could not load native IDN implementation.
.....
...../usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/example_group.rb:530: [BUG] Segmentation fault at 0x00005618a54262ba
ruby 3.3.0dev (2023-11-07 master ced84beb25) [x86_64-linux]

-- Control frame information -----
c:0022 p:0009 s:0108 e:000107 METHOD /usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/example_group.rb:530
c:0021 p:0004 s:0104 e:000102 BLOCK /usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/example_group.rb:536
c:0020 p:0015 s:0099 e:000098 BLOCK /usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/example_group.rb:702 [FINISH]
c:0019 p:---- s:0095 e:000094 CFUNC :each
c:0018 p:0007 s:0091 e:000090 METHOD /usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/example_group.rb:701
c:0017 p:0006 s:0086 e:000085 METHOD /usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/example_group.rb:535
c:0016 p:0026 s:0081 e:000079 METHOD /usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/example_group.rb:556
c:0015 p:0046 s:0075 e:000074 METHOD /usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/example_group.rb:606
c:0014 p:0007 s:0066 e:000065 BLOCK /usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/runner.rb:121 [FINISH]
c:0013 p:---- s:0062 e:000061 CFUNC :map
c:0012 p:0030 s:0058 e:000057 BLOCK /usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/runner.rb:121
c:0011 p:0026 s:0055 e:000054 METHOD /usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/configuration.rb:2070
c:0010 p:0007 s:0051 e:000050 BLOCK /usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/runner.rb:116
c:0009 p:0009 s:0047 e:000046 METHOD /usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/reporter.rb:74
c:0008 p:0019 s:0042 e:000041 METHOD /usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/runner.rb:115
c:0007 p:0035 s:0035 e:000034 METHOD /usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/runner.rb:89
c:0006 p:0058 s:0029 e:000028 METHOD /usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/runner.rb:71
c:0005 p:0013 s:0021 e:000020 METHOD /usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/runner.rb:45
c:0004 p:0010 s:0016 e:000015 TOP /usr/share/gems/gems/rspec-core-3.12.2/exe/rspec:4 [FINISH]
c:0003 p:---- s:0013 e:000012 CFUNC :load
c:0002 p:0078 s:0008 E:001e80 EVAL /usr/bin/rspec:25 [FINISH]
c:0001 p:0000 s:0003 E:000730 DUMMY [FINISH]
```

```

-- Ruby level backtrace information -----
/usr/bin/rspec:25:in `<main>'
/usr/bin/rspec:25:in `load'
/usr/share/gems/gems/rspec-core-3.12.2/exe/rspec:4:in `<top (required)>'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/runner.rb:45:in `invoke'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/runner.rb:71:in `run'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/runner.rb:89:in `run'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/runner.rb:115:in `run_specs'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/reporter.rb:74:in `report'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/runner.rb:116:in `block in run_specs'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/configuration.rb:2070:in `with_suite_hooks'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/runner.rb:121:in `block (2 levels) in run_specs'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/runner.rb:121:in `map'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/runner.rb:121:in `block (3 levels) in run_specs'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/example_group.rb:606:in `run'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/example_group.rb:556:in `run_before_context_hooks'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/example_group.rb:535:in `store_before_context_ivars'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/example_group.rb:701:in `each_instance_variable_for_example'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/example_group.rb:701:in `each'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/example_group.rb:702:in `block in each_instance_variable_for_example'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/example_group.rb:536:in `block in store_before_context_ivars'
/usr/share/gems/gems/rspec-core-3.12.2/lib/rspec/core/example_group.rb:530:in `before_context_ivars'

-- Threading information -----
Total ractor count: 1
Ruby thread count for this ractor: 2

-- Machine register context -----
RIP: 0x00007fe976ebc8e5 RBP: 0x00007ffd7d6c5e80 RSP: 0x00007ffd7d6c5e50
RAX: 0x00007fe9771d5720 RBX: 0xffffffffffffffff RCX: 0x0000000000000000
RDX: 0x0000000000000000 RDI: 0x00005618a54262c2 RSI: 0x0000561dc49e21a0
R8: 0x00000000561dc49e2 R9: 0x0000000000000007 R10: 0x0000561dc49e2b60
R11: 0x0000000000000000 R12: 0x0000561dc49e21d0 R13: 0x00005618a54262b2
R14: 0x0000000000000001 R15: 0x0000561dc49e2090 EFL: 0x0000000000010206

-- C level backtrace information -----
/lib64/libruby.so.3.3(rb_print_backtrace+0x21) [0x7fe9772750a1] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/vm_dump.c:812
/lib64/libruby.so.3.3(rb_vm_bugreport+0x9aa) [0x7fe977277f2a] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/vm_dump.c:1143
/lib64/libruby.so.3.3(rb_bug_for_fatal_signal+0x110) [0x7fe9770d4420] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/error.c:1065
/lib64/libruby.so.3.3(sigsegv+0x56) [0x7fe9771ec576] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/signal.c:920
/lib64/libc.so.6(__restore_rt+0x0) [0x7fe976e5b990]
/lib64/libc.so.6(free+0x25) [0x7fe976ebc8e5]
/lib64/libruby.so.3.3(i_free_name_entry+0x19) [0x7fe9771d5739] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/regparse.c:521
/lib64/libruby.so.3.3(rb_st_foreach+0x85) [0x7fe9771eddd5] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/hash.c:870
/lib64/libruby.so.3.3(onig_names_free+0x27) [0x7fe9771da0c7] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/regparse.c:534
/lib64/libruby.so.3.3(onig_free+0x1a) [0x7fe9771cb86a] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/regcomp.c:5682
/lib64/libruby.so.3.3(obj_free_lto_priv.0+0x3d2) [0x7fe9770ec122] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/gc.c:3611
/lib64/libruby.so.3.3(gc_sweep_page.constprop.0+0x168) [0x7fe9772e9058] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/gc.c:5538

```

```
/lib64/libruby.so.3.3(gc_sweep_step.lto_priv.0+0xf3) [0x7fe9770ea023] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/gc.c:5905
/lib64/libruby.so.3.3(gc_continue+0x34b) [0x7fe9770f249b] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/gc.c:5977
/lib64/libruby.so.3.3(newobj_alloc+0x2de) [0x7fe9770f28be] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/gc.c:2500
/lib64/libruby.so.3.3(rb_wb_protected_newobj_of+0x74) [0x7fe9770f31a4] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/gc.c:2919
/lib64/libruby.so.3.3(rb_hash_new+0x3c) [0x7fe9770ff19c] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/hash.c:1432
/lib64/libruby.so.3.3(vm_exec_core.lto_priv.0+0x30da) [0x7fe97725df9a] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/redhat-linux-build/insns.def:545
/lib64/libruby.so.3.3(rb_vm_exec+0x17d) [0x7fe97727348d] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/vm.c:2472
/lib64/libruby.so.3.3(rb_yield+0x77) [0x7fe977260707] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/vm.c:1622
/lib64/libruby.so.3.3(rb_ary_each+0x44) [0x7fe977062474] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/array.c:2532
/lib64/libruby.so.3.3(vm_call_cfunc_with_frame+0x117) [0x7fe977253b27] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/vm_insnhelper.c:3503
/lib64/libruby.so.3.3(vm_sendish+0xb1) [0x7fe9772560a1] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/vm_insnhelper.c:5585
/lib64/libruby.so.3.3(vm_exec_core.lto_priv.0+0x1f7f) [0x7fe97725ce9f] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/redhat-linux-build/insns.def:802
/lib64/libruby.so.3.3(rb_vm_exec+0x17d) [0x7fe97727348d] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/vm.c:2472
/lib64/libruby.so.3.3(rb_yield+0x77) [0x7fe977260707] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/vm.c:1622
/lib64/libruby.so.3.3(rb_ary_collect.lto_priv.0+0x5c) [0x7fe9770626cc] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/array.c:3624
/lib64/libruby.so.3.3(vm_call_cfunc_with_frame+0x117) [0x7fe977253b27] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/vm_insnhelper.c:3503
/lib64/libruby.so.3.3(vm_sendish+0xb1) [0x7fe9772560a1] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/vm_insnhelper.c:5585
/lib64/libruby.so.3.3(vm_exec_core.lto_priv.0+0x1f7f) [0x7fe97725ce9f] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/redhat-linux-build/insns.def:802
/lib64/libruby.so.3.3(rb_vm_exec+0x17d) [0x7fe97727348d] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/vm.c:2472
/lib64/libruby.so.3.3(rb_load_internal+0x73) [0x7fe977134a63] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/load.c:800
/lib64/libruby.so.3.3(rb_f_load+0xad) [0x7fe977134d4d] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/load.c:875
/lib64/libruby.so.3.3(vm_call_cfunc_with_frame+0x117) [0x7fe977253b27] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/vm_insnhelper.c:3503
/lib64/libruby.so.3.3(vm_exec_core.lto_priv.0+0x16c) [0x7fe97725b08c] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/vm_insnhelper.c:5581
/lib64/libruby.so.3.3(rb_vm_exec+0x17d) [0x7fe97727348d] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/vm.c:2472
/lib64/libruby.so.3.3(rb_ec_exec_node+0xaa) [0x7fe9770dba9a] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/eval.c:287
/lib64/libruby.so.3.3(ruby_run_node+0x93) [0x7fe9770dda53] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/eval.c:328
/usr/bin/ruby-mri(0x561dc3276197) [0x561dc3276197]
/lib64/libc.so.6(__libc_start_call_main+0x7a) [0x7fe976e4514a]
/lib64/libc.so.6(__libc_start_main+0x8b) [0x7fe976e4520b]
/usr/bin/ruby-mri(_start+0x25) [0x561dc32761e5] /usr/src/debug/ruby-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64/main.c:59
```

-- Other runtime information -----

* Process memory map:

561dc3275000-561dc3276000	r--p	00000000	08:08	6714104	/usr/bin/ruby-mri
561dc3276000-561dc3277000	r-xp	00001000	08:08	6714104	/usr/bin/ruby-mri
561dc3277000-561dc3278000	r--p	00002000	08:08	6714104	/usr/bin/ruby-mri
561dc3278000-561dc3279000	r--p	00002000	08:08	6714104	/usr/bin/ruby-mri
561dc3279000-561dc327a000	rw-p	00003000	08:08	6714104	/usr/bin/ruby-mri

561dc34c1000-561dc58f8000	rw-p	00000000	00:00	0	[heap]
7fe94a000000-7fe94bf6a000	r--s	00000000	08:08	6789556	/usr/lib/debug/usr/lib64/
libruby.so.3.3.0-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64.debug					
7fe94c000000-7fe94c021000	rw-p	00000000	00:00	0	
7fe94c021000-7fe950000000	---p	00000000	00:00	0	
7fe952000000-7fe953f6a000	r--s	00000000	08:08	6789556	/usr/lib/debug/usr/lib64/
libruby.so.3.3.0-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64.debug					
7fe954000000-7fe954021000	rw-p	00000000	00:00	0	
7fe954021000-7fe958000000	---p	00000000	00:00	0	
7fe959600000-7fe959851000	r--s	00000000	08:08	6707607	/usr/lib64/libc.so.6
7fe959a00000-7fe959f64000	r--s	00000000	08:08	6788707	/usr/lib64/libruby.so.3.3
.0					
7fe959f8f000-7fe959f90000	---p	00000000	00:00	0	
7fe959f90000-7fe95a7f0000	rw-p	00000000	00:00	0	
7fe95aaa0000-7fe95ac40000	rw-p	00000000	00:00	0	
7fe95ac49000-7fe95ac4d000	r--p	00000000	08:08	6708025	/usr/lib64/libnss_resolve
.so.2					
7fe95ac4d000-7fe95ac69000	r-xp	00004000	08:08	6708025	/usr/lib64/libnss_resolve
.so.2					
7fe95ac69000-7fe95ac71000	r--p	00020000	08:08	6708025	/usr/lib64/libnss_resolve
.so.2					
7fe95ac71000-7fe95ac72000	r--p	00027000	08:08	6708025	/usr/lib64/libnss_resolve
.so.2					
7fe95ac72000-7fe95ac73000	rw-p	00028000	08:08	6708025	/usr/lib64/libnss_resolve
.so.2					
7fe95ac73000-7fe95ac78000	r--p	00000000	08:08	6708024	/usr/lib64/libnss_myhostn
ame.so.2					
7fe95ac78000-7fe95ac8d000	r-xp	00005000	08:08	6708024	/usr/lib64/libnss_myhostn
ame.so.2					
7fe95ac8d000-7fe95ac99000	r--p	0001a000	08:08	6708024	/usr/lib64/libnss_myhostn
ame.so.2					
7fe95ac99000-7fe95ac9e000	r--p	00025000	08:08	6708024	/usr/lib64/libnss_myhostn
ame.so.2					
7fe95ac9e000-7fe95ac9f000	rw-p	0002a000	08:08	6708024	/usr/lib64/libnss_myhostn
ame.so.2					
7fe95ac9f000-7fe95aca0000	---p	00000000	00:00	0	
7fe95aca0000-7fe95b040000	rw-p	00000000	00:00	0	
7fe95b050000-7fe95b410000	rw-p	00000000	00:00	0	
7fe95b41f000-7fe95b421000	r--p	00000000	08:08	6714089	/usr/lib64/libyaml-0.so.2
.0.9					
7fe95b421000-7fe95b43a000	r-xp	00002000	08:08	6714089	/usr/lib64/libyaml-0.so.2
.0.9					
7fe95b43a000-7fe95b43e000	r--p	0001b000	08:08	6714089	/usr/lib64/libyaml-0.so.2
.0.9					
7fe95b43e000-7fe95b43f000	r--p	0001e000	08:08	6714089	/usr/lib64/libyaml-0.so.2
.0.9					
7fe95b43f000-7fe95b570000	rw-p	00000000	00:00	0	
7fe95b571000-7fe95b574000	r--p	00000000	08:08	6789373	/usr/lib64/gems/ruby/bigd
ecimal-3.1.5/bigdecimal.so					
7fe95b574000-7fe95b588000	r-xp	00003000	08:08	6789373	/usr/lib64/gems/ruby/bigd
ecimal-3.1.5/bigdecimal.so					
7fe95b588000-7fe95b58b000	r--p	00017000	08:08	6789373	/usr/lib64/gems/ruby/bigd
ecimal-3.1.5/bigdecimal.so					
7fe95b58b000-7fe95b58c000	r--p	0001a000	08:08	6789373	/usr/lib64/gems/ruby/bigd
ecimal-3.1.5/bigdecimal.so					
7fe95b58c000-7fe95b58d000	rw-p	0001b000	08:08	6789373	/usr/lib64/gems/ruby/bigd
ecimal-3.1.5/bigdecimal.so					
7fe95b58d000-7fe95b591000	r--p	00000000	08:08	6788798	/usr/lib64/ruby/zlib.so
7fe95b591000-7fe95b59b000	r-xp	00004000	08:08	6788798	/usr/lib64/ruby/zlib.so
7fe95b59b000-7fe95b59e000	r--p	0000e000	08:08	6788798	/usr/lib64/ruby/zlib.so
7fe95b59e000-7fe95b59f000	r--p	00010000	08:08	6788798	/usr/lib64/ruby/zlib.so
7fe95b59f000-7fe95b5c0000	rw-p	00000000	00:00	0	
7fe95b5ce000-7fe95b5d5000	r--p	00000000	08:08	6788794	/usr/lib64/ruby/socket.so
7fe95b5d5000-7fe95b5f7000	r-xp	00007000	08:08	6788794	/usr/lib64/ruby/socket.so
7fe95b5f7000-7fe95b5fe000	r--p	00029000	08:08	6788794	/usr/lib64/ruby/socket.so
7fe95b5fe000-7fe95b5ff000	r--p	00030000	08:08	6788794	/usr/lib64/ruby/socket.so
7fe95b5ff000-7fe95b600000	rw-p	00031000	08:08	6788794	/usr/lib64/ruby/socket.so

7fe95b600000-7fe95b780000	rw-p	00000000	00:00	0	
7fe95b790000-7fe95b8a0000	rw-p	00000000	00:00	0	
7fe95b8a6000-7fe95b8a8000	r--p	00000000	08:08	6707981	/usr/lib64/libcap.so.2.48
7fe95b8a8000-7fe95b8ac000	r-xp	00002000	08:08	6707981	/usr/lib64/libcap.so.2.48
7fe95b8ac000-7fe95b8ae000	r--p	00006000	08:08	6707981	/usr/lib64/libcap.so.2.48
7fe95b8ae000-7fe95b8af000	r--p	00007000	08:08	6707981	/usr/lib64/libcap.so.2.48
7fe95b8af000-7fe95b8b0000	rw-p	00008000	08:08	6707981	/usr/lib64/libcap.so.2.48
7fe95b8b0000-7fe95b940000	rw-p	00000000	00:00	0	
7fe95b940000-7fe95b945000	r--s	00000000	08:08	6789371	/usr/lib/debug/usr/bin/ruby-mri-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64.debug
7fe95b945000-7fe95b947000	r--p	00000000	08:08	6788795	/usr/lib64/ruby/stringio.so
7fe95b947000-7fe95b94c000	r-xp	00002000	08:08	6788795	/usr/lib64/ruby/stringio.so
7fe95b94c000-7fe95b94e000	r--p	00007000	08:08	6788795	/usr/lib64/ruby/stringio.so
7fe95b94e000-7fe95b94f000	r--p	00008000	08:08	6788795	/usr/lib64/ruby/stringio.so
7fe95b94f000-7fe95ba10000	rw-p	00000000	00:00	0	
7fe95ba10000-7fe95ba15000	r--s	00000000	08:08	6789371	/usr/lib/debug/usr/bin/ruby-mri-3.3.0~20231107.1312gitced84beb25-183.fc40.283.x86_64.debug
7fe95ba15000-7fe95ba16000	r--p	00000000	08:08	6788784	/usr/lib64/ruby/io/wait.so
7fe95ba16000-7fe95ba17000	r-xp	00001000	08:08	6788784	/usr/lib64/ruby/io/wait.so
7fe95ba17000-7fe95ba18000	r--p	00002000	08:08	6788784	/usr/lib64/ruby/io/wait.so
7fe95ba18000-7fe95ba19000	r--p	00002000	08:08	6788784	/usr/lib64/ruby/io/wait.so
7fe95ba19000-7fe95bala000	rw-p	00000000	00:00	0	
7fe95bala000-7fe95balb000	r--p	00000000	08:08	6788779	/usr/lib64/ruby/erb/escape.so
7fe95balb000-7fe95balc000	r-xp	00001000	08:08	6788779	/usr/lib64/ruby/erb/escape.so
7fe95balc000-7fe95bald000	r--p	00002000	08:08	6788779	/usr/lib64/ruby/erb/escape.so
7fe95bald000-7fe95bale000	r--p	00002000	08:08	6788779	/usr/lib64/ruby/erb/escape.so
7fe95bale000-7fe95balf000	rw-p	00000000	00:00	0	
7fe95balf000-7fe95ba20000	---p	00000000	00:00	0	
7fe95ba20000-7fe95bac1000	rw-p	00000000	00:00	0	
7fe95bac1000-7fe95bac2000	---p	00000000	00:00	0	
7fe95bac2000-7fe95bb63000	rw-p	00000000	00:00	0	
7fe95bb63000-7fe95bb64000	---p	00000000	00:00	0	
7fe95bb64000-7fe95bc05000	rw-p	00000000	00:00	0	
7fe95bc05000-7fe95bc06000	---p	00000000	00:00	0	
7fe95bc06000-7fe95bca7000	rw-p	00000000	00:00	0	
7fe95bca7000-7fe95bca8000	---p	00000000	00:00	0	
7fe95bca8000-7fe95bd49000	rw-p	00000000	00:00	0	
7fe95bd49000-7fe95bd4a000	---p	00000000	00:00	0	
7fe95bd4a000-7fe95bdeb000	rw-p	00000000	00:00	0	
7fe95bdeb000-7fe95bdec000	---p	00000000	00:00	0	
7fe95bdec000-7fe95be8d000	rw-p	00000000	00:00	0	
7fe95be8d000-7fe95be8e000	---p	00000000	00:00	0	
7fe95be8e000-7fe95bf2f000	rw-p	00000000	00:00	0	
7fe95bf2f000-7fe95bf30000	---p	00000000	00:00	0	
7fe95bf30000-7fe95bfd1000	rw-p	00000000	00:00	0	
7fe95bfd1000-7fe95bfd2000	---p	00000000	00:00	0	
7fe95bfd2000-7fe95c073000	rw-p	00000000	00:00	0	
7fe95c073000-7fe95c074000	---p	00000000	00:00	0	
7fe95c074000-7fe95c115000	rw-p	00000000	00:00	0	
7fe95c115000-7fe95c116000	---p	00000000	00:00	0	
7fe95c116000-7fe95c1b7000	rw-p	00000000	00:00	0	
7fe95c1b7000-7fe95c1b8000	---p	00000000	00:00	0	
7fe95c1b8000-7fe95c259000	rw-p	00000000	00:00	0	
7fe95c259000-7fe95c25a000	---p	00000000	00:00	0	
7fe95c25a000-7fe95c2fb000	rw-p	00000000	00:00	0	

7fe95c2fb000-7fe95c2fc000	---	p	00000000	00:00	0	
7fe95c2fc000-7fe95c39d000	rw-	p	00000000	00:00	0	
7fe95c39d000-7fe95c39e000	---	p	00000000	00:00	0	
7fe95c39e000-7fe95c43f000	rw-	p	00000000	00:00	0	
7fe95c43f000-7fe95c440000	---	p	00000000	00:00	0	
7fe95c440000-7fe95c4e1000	rw-	p	00000000	00:00	0	
7fe95c4e1000-7fe95c4e2000	---	p	00000000	00:00	0	
7fe95c4e2000-7fe95c583000	rw-	p	00000000	00:00	0	
7fe95c583000-7fe95c584000	---	p	00000000	00:00	0	
7fe95c584000-7fe95c625000	rw-	p	00000000	00:00	0	
7fe95c625000-7fe95c626000	---	p	00000000	00:00	0	
7fe95c626000-7fe95c6c7000	rw-	p	00000000	00:00	0	
7fe95c6c7000-7fe95c6c8000	---	p	00000000	00:00	0	
7fe95c6c8000-7fe95c769000	rw-	p	00000000	00:00	0	
7fe95c769000-7fe95c76a000	---	p	00000000	00:00	0	
7fe95c76a000-7fe95c80b000	rw-	p	00000000	00:00	0	
7fe95c80b000-7fe95c80c000	---	p	00000000	00:00	0	
7fe95c80c000-7fe95c8ad000	rw-	p	00000000	00:00	0	
7fe95c8ad000-7fe95c8ae000	---	p	00000000	00:00	0	
7fe95c8ae000-7fe95c94f000	rw-	p	00000000	00:00	0	
7fe95c94f000-7fe95c950000	---	p	00000000	00:00	0	
7fe95c950000-7fe95c9f1000	rw-	p	00000000	00:00	0	
7fe95c9f1000-7fe95c9f2000	---	p	00000000	00:00	0	
7fe95c9f2000-7fe95ca93000	rw-	p	00000000	00:00	0	
7fe95ca93000-7fe95ca94000	---	p	00000000	00:00	0	
7fe95ca94000-7fe95cb35000	rw-	p	00000000	00:00	0	
7fe95cb35000-7fe95cb36000	---	p	00000000	00:00	0	
7fe95cb36000-7fe95cbd7000	rw-	p	00000000	00:00	0	
7fe95cbd7000-7fe95cbd8000	---	p	00000000	00:00	0	
7fe95cbd8000-7fe95cc79000	rw-	p	00000000	00:00	0	
7fe95cc79000-7fe95cc7a000	---	p	00000000	00:00	0	
7fe95cc7a000-7fe95cd1b000	rw-	p	00000000	00:00	0	
7fe95cd1b000-7fe95cd1c000	---	p	00000000	00:00	0	
7fe95cd1c000-7fe95cdbd000	rw-	p	00000000	00:00	0	
7fe95cdbd000-7fe95cdbe000	---	p	00000000	00:00	0	
7fe95cdbe000-7fe95ce5f000	rw-	p	00000000	00:00	0	
7fe95ce5f000-7fe95ce60000	---	p	00000000	00:00	0	
7fe95ce60000-7fe95d6b0000	rw-	p	00000000	00:00	0	
7fe95d6b0000-7fe95d6b2000	r--	p	00000000	08:08	6788796	/usr/lib64/ruby/strscan.so
7fe95d6b2000-7fe95d6b5000	r-x	p	00002000	08:08	6788796	/usr/lib64/ruby/strscan.so
7fe95d6b5000-7fe95d6b6000	r--	p	00005000	08:08	6788796	/usr/lib64/ruby/strscan.so
7fe95d6b6000-7fe95d6b7000	r--	p	00006000	08:08	6788796	/usr/lib64/ruby/strscan.so
7fe95d6b7000-7fe95d6b8000	rw-	p	00000000	00:00	0	
7fe95d6b8000-7fe95d6ba000	r--	p	00000000	08:08	6788708	/usr/lib64/ruby/cgi/escape.so
7fe95d6ba000-7fe95d6bc000	r-x	p	00002000	08:08	6788708	/usr/lib64/ruby/cgi/escape.so
7fe95d6bc000-7fe95d6bd000	r--	p	00004000	08:08	6788708	/usr/lib64/ruby/cgi/escape.so
7fe95d6bd000-7fe95d6be000	r--	p	00004000	08:08	6788708	/usr/lib64/ruby/cgi/escape.so
7fe95d6be000-7fe976abf000	rw-	p	00000000	00:00	0	
7fe976ac2000-7fe976ac6000	r--	s	00000000	08:08	6714104	/usr/bin/ruby-mri
7fe976ac6000-7fe976ac9000	r--	p	00000000	08:08	6714117	/usr/lib64/gems/ruby/psych-5.1.1.1/psych.so
7fe976ac9000-7fe976acd000	r-x	p	00003000	08:08	6714117	/usr/lib64/gems/ruby/psych-5.1.1.1/psych.so
7fe976acd000-7fe976ace000	r--	p	00007000	08:08	6714117	/usr/lib64/gems/ruby/psych-5.1.1.1/psych.so
7fe976ace000-7fe976acf000	r--	p	00008000	08:08	6714117	/usr/lib64/gems/ruby/psych-5.1.1.1/psych.so
7fe976acf000-7fe976b30000	rw-	p	00000000	00:00	0	
7fe976b32000-7fe976b33000	r--	p	00000000	08:08	6788785	/usr/lib64/ruby/monitor.so

```

o
7fe976b33000-7fe976b34000 r-xp 00001000 08:08 6788785 /usr/lib64/ruby/monitor.s
o
7fe976b34000-7fe976b35000 r--p 00002000 08:08 6788785 /usr/lib64/ruby/monitor.s
o
7fe976b35000-7fe976b36000 r--p 00002000 08:08 6788785 /usr/lib64/ruby/monitor.s
o
7fe976b36000-7fe976b37000 rw-p 00000000 00:00 0
7fe976b37000-7fe976b38000 r--p 00000000 08:08 6788765 /usr/lib64/ruby/enc/trans
/transdb.so
7fe976b38000-7fe976b39000 r-xp 00001000 08:08 6788765 /usr/lib64/ruby/enc/trans
/transdb.so
7fe976b39000-7fe976b3a000 r--p 00002000 08:08 6788765 /usr/lib64/ruby/enc/trans
/transdb.so
7fe976b3a000-7fe976b3b000 r--p 00002000 08:08 6788765 /usr/lib64/ruby/enc/trans
/transdb.so
7fe976b3b000-7fe976c3d000 rw-p 00000000 00:00 0
7fe976c3d000-7fe976c96000 r--p 00000000 08:08 6707590 /usr/lib/locale/C.utf8/LC
_CTYPE
7fe976c96000-7fe976ca6000 r--p 00000000 08:08 6707610 /usr/lib64/libm.so.6
7fe976ca6000-7fe976d1c000 r-xp 00010000 08:08 6707610 /usr/lib64/libm.so.6
7fe976d1c000-7fe976d76000 r--p 00086000 08:08 6707610 /usr/lib64/libm.so.6
7fe976d76000-7fe976d77000 r--p 000df000 08:08 6707610 /usr/lib64/libm.so.6
7fe976d77000-7fe976d78000 rw-p 000e0000 08:08 6707610 /usr/lib64/libm.so.6
7fe976d78000-7fe976d89000 r--p 00000000 08:08 6707959 /usr/lib64/libgmp.so.10.4
.1
7fe976d89000-7fe976e05000 r-xp 00011000 08:08 6707959 /usr/lib64/libgmp.so.10.4
.1
7fe976e05000-7fe976e1a000 r--p 0008d000 08:08 6707959 /usr/lib64/libgmp.so.10.4
.1
7fe976e1a000-7fe976e1c000 r--p 000a1000 08:08 6707959 /usr/lib64/libgmp.so.10.4
.1
7fe976e1c000-7fe976e1d000 rw-p 000a3000 08:08 6707959 /usr/lib64/libgmp.so.10.4
.1
7fe976e1d000-7fe976e43000 r--p 00000000 08:08 6707607 /usr/lib64/libc.so.6
7fe976e43000-7fe976fa4000 r-xp 00026000 08:08 6707607 /usr/lib64/libc.so.6
7fe976fa4000-7fe976ff2000 r--p 00187000 08:08 6707607 /usr/lib64/libc.so.6
7fe976ff2000-7fe976ff6000 r--p 001d4000 08:08 6707607 /usr/lib64/libc.so.6
7fe976ff6000-7fe976ff8000 rw-p 001d8000 08:08 6707607 /usr/lib64/libc.so.6
7fe976ff8000-7fe977000000 rw-p 00000000 00:00 0
7fe977000000-7fe977049000 r--p 00000000 08:08 6788707 /usr/lib64/libruby.so.3.3
.0
7fe977049000-7fe9773bf000 r-xp 00049000 08:08 6788707 /usr/lib64/libruby.so.3.3
.0
7fe9773bf000-7fe977527000 r--p 003bf000 08:08 6788707 /usr/lib64/libruby.so.3.3
.0
7fe977527000-7fe977540000 r--p 00526000 08:08 6788707 /usr/lib64/libruby.so.3.3
.0
7fe977540000-7fe977541000 rw-p 0053f000 08:08 6788707 /usr/lib64/libruby.so.3.3
.0
7fe977541000-7fe977556000 rw-p 00000000 00:00 0
7fe977559000-7fe97755a000 r--p 00000000 08:08 6788722 /usr/lib64/ruby/enc/encdb
.so
7fe97755a000-7fe97755b000 r-xp 00001000 08:08 6788722 /usr/lib64/ruby/enc/encdb
.so
7fe97755b000-7fe97755c000 r--p 00002000 08:08 6788722 /usr/lib64/ruby/enc/encdb
.so
7fe97755c000-7fe97755d000 r--p 00002000 08:08 6788722 /usr/lib64/ruby/enc/encdb
.so
7fe97755d000-7fe97755e000 rw-p 00000000 00:00 0
7fe97755e000-7fe977565000 r--s 00000000 08:08 6707673 /usr/lib64/gconv/gconv-mo
dules.cache
7fe977565000-7fe977568000 rw-p 00000000 00:00 0
7fe977568000-7fe97756b000 r--p 00000000 08:08 6706024 /usr/lib64/libgcc_s-13-20
231011.so.1
7fe97756b000-7fe977586000 r-xp 00003000 08:08 6706024 /usr/lib64/libgcc_s-13-20
231011.so.1

```

```

7fe977586000-7fe97758a000 r--p 0001e000 08:08 6706024 /usr/lib64/libgcc_s-13-20
231011.so.1
7fe97758a000-7fe97758b000 r--p 00021000 08:08 6706024 /usr/lib64/libgcc_s-13-20
231011.so.1
7fe97758b000-7fe97758e000 rw-p 00000000 00:00 0
7fe97758e000-7fe977590000 r--p 00000000 08:08 6707999 /usr/lib64/libcrypt.so.2.
0.0
7fe977590000-7fe9775a4000 r-xp 00002000 08:08 6707999 /usr/lib64/libcrypt.so.2.
0.0
7fe9775a4000-7fe9775bd000 r--p 00016000 08:08 6707999 /usr/lib64/libcrypt.so.2.
0.0
7fe9775bd000-7fe9775be000 r--p 0002e000 08:08 6707999 /usr/lib64/libcrypt.so.2.
0.0
7fe9775be000-7fe9775c7000 rw-p 00000000 00:00 0
7fe9775c7000-7fe9775ca000 r--p 00000000 08:08 6707836 /usr/lib64/libz.so.1.2.13
7fe9775ca000-7fe9775d9000 r-xp 00003000 08:08 6707836 /usr/lib64/libz.so.1.2.13
7fe9775d9000-7fe9775df000 r--p 00012000 08:08 6707836 /usr/lib64/libz.so.1.2.13
7fe9775df000-7fe9775e0000 r--p 00018000 08:08 6707836 /usr/lib64/libz.so.1.2.13
7fe9775e0000-7fe9775e3000 rw-p 00000000 00:00 0
7fe9775e6000-7fe9775e7000 r--p 00000000 08:08 6707604 /usr/lib64/ld-linux-x86-6
4.so.2
7fe9775e7000-7fe97760e000 r-xp 00001000 08:08 6707604 /usr/lib64/ld-linux-x86-6
4.so.2
7fe97760e000-7fe977618000 r--p 00028000 08:08 6707604 /usr/lib64/ld-linux-x86-6
4.so.2
7fe977618000-7fe97761a000 r--p 00031000 08:08 6707604 /usr/lib64/ld-linux-x86-6
4.so.2
7fe97761a000-7fe97761c000 rw-p 00033000 08:08 6707604 /usr/lib64/ld-linux-x86-6
4.so.2
7ffd7cec9000-7ffd7d6c8000 rw-p 00000000 00:00 0 [stack]
7ffd7d7c9000-7ffd7d7cd000 r--p 00000000 00:00 0 [vvar]
7ffd7d7cd000-7ffd7d7cf000 r-xp 00000000 00:00 0 [vdso]
ffffffff600000-ffffffff601000 --xp 00000000 00:00 0 [vsyscall]

```

Aborted (core dumped)

Looks like running testsuite brings about GC for ruby regex and it seems to cause segfault.

valgrind says:

```

==93== Invalid free() / delete / delete[] / realloc()
==93==    at 0x4845B2C: free (vg_replace_malloc.c:985)
==93==    by 0x4A2E738: i_free_name_entry (regparse.c:521)
==93==    by 0x4A46DD4: UnknownInlinedFun (hash.c:870)
==93==    by 0x4A46DD4: UnknownInlinedFun (st.c:1516)
==93==    by 0x4A46DD4: rb_st_foreach (st.c:1613)
==93==    by 0x4A330C6: UnknownInlinedFun (regparse.c:534)
==93==    by 0x4A330C6: onig_names_free (regparse.c:545)
==93==    by 0x4A24869: UnknownInlinedFun (regcomp.c:5682)
==93==    by 0x4A24869: onig_free (regcomp.c:5679)
==93==    by 0x4945121: obj_free.lto_priv.0 (gc.c:3611)
==93==    by 0x4B42057: UnknownInlinedFun (gc.c:5538)
==93==    by 0x4B42057: gc_sweep_page.constprop.0 (gc.c:5623)
==93==    by 0x4943022: gc_sweep_step.lto_priv.0 (gc.c:5905)
==93==    by 0x494B49A: UnknownInlinedFun (gc.c:5977)
==93==    by 0x494B49A: gc_continue (gc.c:2488)
==93==    by 0x494B8BD: UnknownInlinedFun (gc.c:2500)
==93==    by 0x494B8BD: UnknownInlinedFun (gc.c:2715)
==93==    by 0x494B8BD: newobj_alloc (gc.c:2816)
==93==    by 0x494C1A3: UnknownInlinedFun (gc.c:2919)
==93==    by 0x494C1A3: UnknownInlinedFun (gc.c:2936)
==93==    by 0x494C1A3: rb_wb_protected_newobj_of (gc.c:2951)
==93==    by 0x495819B: UnknownInlinedFun (hash.c:1432)
==93==    by 0x495819B: UnknownInlinedFun (hash.c:1443)
==93==    by 0x495819B: rb_hash_new (hash.c:1457)
==93== Address 0x223e3ec0 is 0 bytes inside a block of size 6 free'd

```

```

==93== at 0x4845B2C: free (vg_replace_malloc.c:985)
==93== by 0x4A2E738: i_free_name_entry (regparse.c:521)
==93== by 0x4A46DD4: UnknownInlinedFun (hash.c:870)
==93== by 0x4A46DD4: UnknownInlinedFun (st.c:1516)
==93== by 0x4A46DD4: rb_st_foreach (st.c:1613)
==93== by 0x4A330C6: UnknownInlinedFun (regparse.c:534)
==93== by 0x4A330C6: onig_names_free (regparse.c:545)
==93== by 0x4A24869: UnknownInlinedFun (regcomp.c:5682)
==93== by 0x4A24869: onig_free (regcomp.c:5679)
==93== by 0x4945121: obj_free.lto_priv.0 (gc.c:3611)
==93== by 0x4B42057: UnknownInlinedFun (gc.c:5538)
==93== by 0x4B42057: gc_sweep_page.constprop.0 (gc.c:5623)
==93== by 0x4943022: gc_sweep_step.lto_priv.0 (gc.c:5905)
==93== by 0x494B49A: UnknownInlinedFun (gc.c:5977)
==93== by 0x494B49A: gc_continue (gc.c:2488)
==93== by 0x494B8BD: UnknownInlinedFun (gc.c:2500)
==93== by 0x494B8BD: UnknownInlinedFun (gc.c:2715)
==93== by 0x494B8BD: newobj_alloc (gc.c:2816)
==93== by 0x494C1A3: UnknownInlinedFun (gc.c:2919)
==93== by 0x494C1A3: UnknownInlinedFun (gc.c:2936)
==93== by 0x494C1A3: rb_wb_protected_newobj_of (gc.c:2951)
==93== by 0x495819B: UnknownInlinedFun (hash.c:1432)
==93== by 0x495819B: UnknownInlinedFun (hash.c:1443)
==93== by 0x495819B: rb_hash_new (hash.c:1457)
==93== Block was alloc'd at
==93== at 0x484280F: malloc (vg_replace_malloc.c:442)
==93== by 0x4A3AFA9: UnknownInlinedFun (regparse.c:287)
==93== by 0x4A3AFA9: UnknownInlinedFun (regparse.c:887)
==93== by 0x4A3AFA9: UnknownInlinedFun (regparse.c:5150)
==93== by 0x4A3AFA9: parse_exp (regparse.c:6227)
==93== by 0x4A3B1E6: parse_branch (regparse.c:6585)
==93== by 0x4A3B477: parse_subexp (regparse.c:6646)
==93== by 0x4A39C1A: UnknownInlinedFun (regparse.c:5074)
==93== by 0x4A39C1A: parse_exp (regparse.c:6227)
==93== by 0x4A3B2D4: parse_branch (regparse.c:6598)
==93== by 0x4A3B396: parse_subexp (regparse.c:6631)
==93== by 0x4A3B5DD: UnknownInlinedFun (regparse.c:6680)
==93== by 0x4A3B5DD: onig_parse_make_tree (regparse.c:6725)
==93== by 0x4A24B5E: onig_compile_ruby (regcomp.c:5866)
==93== by 0x4A18AA7: UnknownInlinedFun (re.c:876)
==93== by 0x4A18AA7: UnknownInlinedFun (re.c:900)
==93== by 0x4A18AA7: rb_reg_initialize (re.c:3265)
==93== by 0x4A18D0C: rb_reg_initialize_str (re.c:3299)
==93== by 0x4A18E0E: rb_reg_init_str (re.c:3334)

```

so looks like this is double-free. Currently I am unable to create minimum reproducer.

History

#1 - 11/07/2023 09:28 PM - HParker (Adam Hess)

This should be fixed by this PR: <https://github.com/ruby/ruby/pull/8813>

The easy reproduction is

```

10_000.times do
  Regexp.new(Regexp.new("(?<name> ") )
end

```

#2 - 11/08/2023 04:16 AM - nobu (Nobuyoshi Nakada)

@HParker Could you add the test to the PR?

#3 - 11/08/2023 06:55 AM - HParker (Adam Hess)

Updated! let me know how it looks. I just used the reproduction script directly as the test.

#4 - 11/08/2023 01:06 PM - peterzhu2118 (Peter Zhu)

- Status changed from Open to Closed

I've merged the PR, so I will be closing this issue. Thank you for reporting it!

#5 - 11/08/2023 03:08 PM - mtasaka (Mamoru TASAKA)

Confirmed fixed for the test case of rubygem-addressable, thank you!