Ruby trunk - Bug #15245

Heap buffer overflow (write of size 8) in vm.inc

10/23/2018 04:46 PM - bannable (Joe Truba)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.6.0dev (2018-10-16 trunk 65097) [x86_64-linux]	**Backport:**	2.3: DONTNEED, 2.4: DONTNEED, 2.5: DONE

Description

Reproducer:

```
$ xxd repro1_2
00000000: 2557 0030 007c 7c30 7768 696c 650a 30    %W.0.||0while.0
$
```

AddressSanitizer report:

```
=================================================================
==43391==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62d000d13fd8 at pc 0x55713d1d5
cab bp 0x7ffe42230070 sp 0x7ffe42230068
WRITE of size 8 at 0x62d000d13fd8 thread T0
    #0 0x55713d1d5caa in vm_exec_core /home/jtruba/rubies/ruby-trunk-asan/vm.inc:797:13
    #1 0x55713d213dd4 in rb_vm_exec /home/jtruba/rubies/ruby-trunk-asan/vm.c
    #2 0x55713cc28286 in ruby_exec_internal /home/jtruba/rubies/ruby-trunk-asan/eval.c:261:2
    #3 0x55713cc28286 in ruby_exec_node /home/jtruba/rubies/ruby-trunk-asan/eval.c:325
    #4 0x55713cc27ca5 in ruby_run_node /home/jtruba/rubies/ruby-trunk-asan/eval.c:317:25
    #5 0x55713cc1e960 in main /home/jtruba/rubies/ruby-trunk-asan/./main.c:42:9
    #6 0x7fdd2f340b44 in __libc_start_main /build/glibc-6V9RKT/glibc-2.19/csu/libc-start.c:287
    #7 0x55713cb4873b in _start (/home/jtruba/rubies/ruby-trunk-asan/ruby+0x13b73b)

0x62d000d13fd8 is located 0 bytes to the right of 16344-byte region [0x62d000d10000,0x62d000d13fd8
)
allocated by thread T0 here:
    #0 0x55713cbf07fe in __interceptor_posix_memalign /home/jtruba/to_install/llvm/llvm/projects/c
ompiler-rt/lib/asan/asan_malloc_linux.cc:167:3
    #1 0x55713cc9bc7d in aligned_malloc /home/jtruba/rubies/ruby-trunk-asan/gc.c:7806:9
    #2 0x55713cc9bc7d in heap_page_allocate /home/jtruba/rubies/ruby-trunk-asan/gc.c:1527
    #3 0x55713cc9bc7d in heap_page_create /home/jtruba/rubies/ruby-trunk-asan/gc.c:1628
    #4 0x55713cc9bc7d in heap_assign_page /home/jtruba/rubies/ruby-trunk-asan/gc.c:1648
    #5 0x55713cc8da80 in heap_increment /home/jtruba/rubies/ruby-trunk-asan/gc.c:1729:2
    #6 0x55713cc8da80 in heap_prepare /home/jtruba/rubies/ruby-trunk-asan/gc.c:1748
    #7 0x55713cc8da80 in heap_get_freeobj_from_next_freepage /home/jtruba/rubies/ruby-trunk-asan/g
c.c:1761
    #8 0x55713cc8da80 in heap_get_freeobj /home/jtruba/rubies/ruby-trunk-asan/gc.c:1795
    #9 0x55713cc8da80 in newobj_slowpath /home/jtruba/rubies/ruby-trunk-asan/gc.c:1925
    #10 0x55713cc8c755 in newobj_slowpath_wb_protected /home/jtruba/rubies/ruby-trunk-asan/gc.c:19
37:12

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/jtruba/rubies/ruby-trunk-asan/vm.inc:797:13
in vm_exec_core
Shadow bytes around the buggy address:
  0x0c5a8019a7a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5a8019a7b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5a8019a7c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5a8019a7d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5a8019a7e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c5a8019a7f0: 00 00 00 00 00 00 00 00 00 00[fa]fa fa fa fa
  0x0c5a8019a800: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5a8019a810: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5a8019a820: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
  0x0c5a8019a830: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5a8019a840: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==43391==ABORTING
```

Crash dump:

```
jtruba@dev118:~/rubies/ruby-trunk$ ./ruby ../repro1_2




                          [63/3534]
../repro1_2:1: [BUG] gc_sweep(): unknown data type 0x18(0x00007f9663544038) 0x7f966355abb8
ruby 2.6.0dev (2018-10-16 trunk 65097) [x86_64-linux]

-- Control frame information -----------------------------------------------
c:0002 p:0004 s:-1458793 e:000005 EVAL   ../repro1_2:1 [FINISH]
c:0001 p:0000 s:0003 E:001cf0 (none) [FINISH]

-- Ruby level backtrace information ----------------------------------------
../repro1_2:1:in `<main>'

-- C level backtrace information -------------------------------------------
./ruby(0x55d8d3e4f7c0) [0x55d8d3e4f7c0]
/home/jtruba/rubies/ruby-trunk/ruby(rb_vm_bugreport) vm_dump.c:985
/home/jtruba/rubies/ruby-trunk/ruby(bug_report_end+0x0) [0x55d8d3e2a2cc] error.c:27072
/home/jtruba/rubies/ruby-trunk/ruby(rb_bug) error.c:595
./ruby(0x55d8d39a8459) [0x55d8d39a8459]
./ruby(0x55d8d39a6242) [0x55d8d39a6242]
./ruby(0x55d8d39a3b6f) [0x55d8d39a3b6f]
./ruby(0x55d8d39a3257) [0x55d8d39a3257]
/home/jtruba/rubies/ruby-trunk/ruby(ibf_dump_write+0x4e) [0x55d8d3987503] gc.c:41745
/home/jtruba/rubies/ruby-trunk/ruby(newobj_of) compile.c:9455
/home/jtruba/rubies/ruby-trunk/ruby(rb_wb_protected_newobj_of) gc.c:1990
./ruby(rb_str_resurrect+0xd) [0x55d8d3bcad54]
/home/jtruba/rubies/ruby-trunk/ruby(rb_str_resurrect) string.c:1499
./ruby(0x55d8d3ca7f68) [0x55d8d3ca7f68]
./ruby(rb_vm_exec+0x1884) [0x55d8d3cc8504]
./ruby(rb_iseq_eval_main+0x536) [0x55d8d3cc8f76]
./ruby(ruby_exec_node+0x46) [0x55d8d3969499]
/home/jtruba/rubies/ruby-trunk/ruby(rb_check_lockedtmp) compile.c:5878
/home/jtruba/rubies/ruby-trunk/ruby(str_modifiable) string.c:2027
/home/jtruba/rubies/ruby-trunk/ruby(str_independent) string.c:2045
/home/jtruba/rubies/ruby-trunk/ruby(str_modify_keep_cr) string.c:2114
/home/jtruba/rubies/ruby-trunk/ruby(parser_peek_variable_name) string.c:5664
/home/jtruba/rubies/ruby-trunk/ruby(parse_string) parse.y:5927
/home/jtruba/rubies/ruby-trunk/ruby(io_fd_check_closed) parse.y:7603
/home/jtruba/rubies/ruby-trunk/ruby(rb_io_check_closed) io.c:647
/home/jtruba/rubies/ruby-trunk/ruby(io_fd_check_closed) io.c:6100
```

```
/home/jtruba/rubies/ruby-trunk/ruby(rb_io_check_closed) io.c:647
/home/jtruba/rubies/ruby-trunk/ruby(io_strip_bom) io.c:6034
/home/jtruba/rubies/ruby-trunk/ruby(ruby_exec_node) io.c:6097
./ruby(ruby_run_node+0x3c) [0x55d8d39691e8]
/home/jtruba/rubies/ruby-trunk/ruby(compile_data_alloc_adjust) compile.c:882
/home/jtruba/rubies/ruby-trunk/ruby(new_adjust_body) compile.c:1116
/home/jtruba/rubies/ruby-trunk/ruby(compile_break) compile.c:5375
/home/jtruba/rubies/ruby-trunk/ruby(RUBY_VM_CONTROL_FRAME_STACK_OVERFLOW_P) compile.c:5898
/home/jtruba/rubies/ruby-trunk/ruby(rb_source_location) vm.c:519
/home/jtruba/rubies/ruby-trunk/ruby(parse_ident) vm.c:1310
/home/jtruba/rubies/ruby-trunk/ruby(ruby_run_node) parse.y:8255
/home/jtruba/rubies/ruby-trunk/ruby(rb_array_len+0x3) [0x55d8d3963e18] ./main.c:1087
/home/jtruba/rubies/ruby-trunk/ruby(ary_tmp_hash_new) array.c:4132
/home/jtruba/rubies/ruby-trunk/ruby(ary_make_hash) array.c:4142
/home/jtruba/rubies/ruby-trunk/ruby(str_independent) array.c:4602
/home/jtruba/rubies/ruby-trunk/ruby(main) string.c:5422
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf5) [0x7f9664b08b45] libc-start.c:287
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main) (null):0
./ruby(0x55d8d3963c79) [0x55d8d3963c79]
/home/jtruba/rubies/ruby-trunk/ruby(compile_data_alloc_insn) compile.c:870
/home/jtruba/rubies/ruby-trunk/ruby(new_insn_core) compile.c:1129
/home/jtruba/rubies/ruby-trunk/ruby(new_insn_body) compile.c:1159
/home/jtruba/rubies/ruby-trunk/ruby(vm_push_frame) compile.c:6568
/home/jtruba/rubies/ruby-trunk/ruby(vm_set_eval_stack) vm.c:478

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

* Loaded script: ../repro1_2

* Loaded features:

    0 enumerator.so
    1 thread.rb
    2 rational.so
    3 complex.so
    4 /home/jtruba/.rubies/ruby-trunk/lib/ruby/2.6.0/x86_64-linux/enc/encdb.so
    5 /home/jtruba/.rubies/ruby-trunk/lib/ruby/2.6.0/x86_64-linux/enc/trans/transdb.so

* Process memory map:

55d8d393b000-55d8d3f40000 r-xp 00000000 103:00 78003143                   /home/jtruba/rubies/ruby-
trunk/ruby
55d8d413f000-55d8d4145000 rw-p 00604000 103:00 78003143                   /home/jtruba/rubies/ruby-
trunk/ruby
55d8d4145000-55d8d4167000 rw-p 00000000 00:00 0
7f9662242000-7f96631ea000 r--s 00000000 103:00 78003143                   /home/jtruba/rubies/ruby-
trunk/ruby
7f96631ea000-7f9663200000 r-xp 00000000 103:03 786893                     /lib/x86_64-linux-gnu/lib
gcc_s.so.1
7f9663200000-7f96633ff000 ---p 00016000 103:03 786893                     /lib/x86_64-linux-gnu/lib
gcc_s.so.1
7f96633ff000-7f9663400000 rw-p 00015000 103:03 786893                     /lib/x86_64-linux-gnu/lib
gcc_s.so.1
7f9663400000-7f9663c00000 rw-p 00000000 00:00 0
7f9663c54000-7f9663dfd000 r--s 00000000 103:03 786457                     /lib/x86_64-linux-gnu/lib
c-2.19.so
7f9663dfd000-7f9663dff000 r-xp 00000000 103:00 80759003                   /home/jtruba/.rubies/ruby
-trunk/lib/ruby/2.6.0/x86_64-linux/enc/trans/transdb.so
7f9663dff000-7f9663fff000 ---p 00002000 103:00 80759003                   /home/jtruba/.rubies/ruby
-trunk/lib/ruby/2.6.0/x86_64-linux/enc/trans/transdb.so
7f9663fff000-7f9664000000 rw-p 00002000 103:00 80759003                   /home/jtruba/.rubies/ruby
-trunk/lib/ruby/2.6.0/x86_64-linux/enc/trans/transdb.so
7f9664000000-7f9664800000 rw-p 00000000 00:00 0
7f96648e5000-7f96648e7000 r-xp 00000000 103:00 80759038                   /home/jtruba/.rubies/ruby
-trunk/lib/ruby/2.6.0/x86_64-linux/enc/encdb.so
7f96648e7000-7f9664ae6000 ---p 00002000 103:00 80759038                   /home/jtruba/.rubies/ruby
-trunk/lib/ruby/2.6.0/x86_64-linux/enc/encdb.so
```

```
7f9664ae6000-7f9664ae7000 rw-p 00001000 103:00 80759038                   /home/jtruba/.rubies/ruby
-trunk/lib/ruby/2.6.0/x86_64-linux/enc/encdb.so
7f9664ae7000-7f9664c88000 r-xp 00000000 103:03 786457                     /lib/x86_64-linux-gnu/lib
c-2.19.so
7f9664c88000-7f9664e88000 ---p 001a1000 103:03 786457                     /lib/x86_64-linux-gnu/lib
c-2.19.so
7f9664e88000-7f9664e8c000 r--p 001a1000 103:03 786457                     /lib/x86_64-linux-gnu/lib
c-2.19.so
7f9664e8c000-7f9664e8e000 rw-p 001a5000 103:03 786457                     /lib/x86_64-linux-gnu/lib
c-2.19.so
7f9664e8e000-7f9664e92000 rw-p 00000000 00:00 0
7f9664e92000-7f9664f92000 r-xp 00000000 103:03 786463                     /lib/x86_64-linux-gnu/lib
m-2.19.so
7f9664f92000-7f9665191000 ---p 00100000 103:03 786463                     /lib/x86_64-linux-gnu/lib
m-2.19.so
7f9665191000-7f9665192000 r--p 000ff000 103:03 786463                     /lib/x86_64-linux-gnu/lib
m-2.19.so
7f9665192000-7f9665193000 rw-p 00100000 103:03 786463                     /lib/x86_64-linux-gnu/lib
m-2.19.so
7f9665193000-7f966519b000 r-xp 00000000 103:03 786461                     /lib/x86_64-linux-gnu/lib
crypt-2.19.so
7f966519b000-7f966539a000 ---p 00008000 103:03 786461                     /lib/x86_64-linux-gnu/lib
crypt-2.19.so
7f966539a000-7f966539b000 r--p 00007000 103:03 786461                     /lib/x86_64-linux-gnu/lib
crypt-2.19.so
7f966539b000-7f966539c000 rw-p 00008000 103:03 786461                     /lib/x86_64-linux-gnu/lib
crypt-2.19.so
7f966539c000-7f96653ca000 rw-p 00000000 00:00 0
7f96653ca000-7f96653cd000 r-xp 00000000 103:03 786462                     /lib/x86_64-linux-gnu/lib
dl-2.19.so
7f96653cd000-7f96655cc000 ---p 00003000 103:03 786462                     /lib/x86_64-linux-gnu/lib
dl-2.19.so
7f96655cc000-7f96655cd000 r--p 00002000 103:03 786462                     /lib/x86_64-linux-gnu/lib
dl-2.19.so
7f96655cd000-7f96655ce000 rw-p 00003000 103:03 786462                     /lib/x86_64-linux-gnu/lib
dl-2.19.so
7f96655ce000-7f966564f000 r-xp 00000000 103:03 266462                     /usr/lib/x86_64-linux-gnu
/libgmp.so.10.2.0
7f966564f000-7f966584f000 ---p 00081000 103:03 266462                     /usr/lib/x86_64-linux-gnu
/libgmp.so.10.2.0
7f966584f000-7f9665850000 r--p 00081000 103:03 266462                     /usr/lib/x86_64-linux-gnu
/libgmp.so.10.2.0
7f9665850000-7f9665851000 rw-p 00082000 103:03 266462                     /usr/lib/x86_64-linux-gnu
/libgmp.so.10.2.0
7f9665851000-7f9665885000 r-xp 00000000 103:03 279726                     /usr/lib/x86_64-linux-gnu
/libjemalloc.so.1
7f9665885000-7f9665a85000 ---p 00034000 103:03 279726                     /usr/lib/x86_64-linux-gnu
/libjemalloc.so.1
7f9665a85000-7f9665a87000 r--p 00034000 103:03 279726                     /usr/lib/x86_64-linux-gnu
/libjemalloc.so.1
7f9665a87000-7f9665a88000 rw-p 00036000 103:03 279726                     /usr/lib/x86_64-linux-gnu
/libjemalloc.so.1
7f9665a88000-7f9665a89000 rw-p 00000000 00:00 0
7f9665a89000-7f9665a90000 r-xp 00000000 103:03 786474                     /lib/x86_64-linux-gnu/lib
rt-2.19.so
7f9665a90000-7f9665c8f000 ---p 00007000 103:03 786474                     /lib/x86_64-linux-gnu/lib
rt-2.19.so
7f9665c8f000-7f9665c90000 r--p 00006000 103:03 786474                     /lib/x86_64-linux-gnu/lib
rt-2.19.so
7f9665c90000-7f9665c91000 rw-p 00007000 103:03 786474                     /lib/x86_64-linux-gnu/lib
rt-2.19.so
7f9665c91000-7f9665ca9000 r-xp 00000000 103:03 786451                     /lib/x86_64-linux-gnu/lib
pthread-2.19.so
7f9665ca9000-7f9665ea8000 ---p 00018000 103:03 786451                     /lib/x86_64-linux-gnu/lib
pthread-2.19.so
7f9665ea8000-7f9665ea9000 r--p 00017000 103:03 786451                     /lib/x86_64-linux-gnu/lib
pthread-2.19.so
```

```
7f9665ea9000-7f9665eaa000 rw-p 00018000 103:03 786451                    /lib/x86_64-linux-gnu/lib
pthread-2.19.so
7f9665eaa000-7f9665eae000 rw-p 00000000 00:00 0
7f9665eae000-7f9665ecf000 r-xp 00000000 103:03 786452                    /lib/x86_64-linux-gnu/ld-
2.19.so
7f9665f2c000-7f96660b5000 r--p 00000000 103:03 283083                    /usr/lib/locale/locale-ar
chive
7f96660b5000-7f96660bb000 rw-p 00000000 00:00 0
7f96660cb000-7f96660cc000 rw-p 00000000 00:00 0
7f96660cc000-7f96660ce000 rw-p 00000000 00:00 0
7f96660ce000-7f96660cf000 r--p 00020000 103:03 786452                    /lib/x86_64-linux-gnu/ld-
2.19.so
7f96660cf000-7f96660d0000 rw-p 00021000 103:03 786452                    /lib/x86_64-linux-gnu/ld-
2.19.so
7f96660d0000-7f96660d1000 rw-p 00000000 00:00 0
7fff921b5000-7fff929b4000 rw-p 00000000 00:00 0                          [stack]
7fff929f4000-7fff929f6000 r--p 00000000 00:00 0                          [vvar]
7fff929f6000-7fff929f8000 r-xp 00000000 00:00 0                          [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0                  [vsyscall]


[NOTE]
You may have encountered a bug in the Ruby interpreter or extension libraries.
Bug reports are welcome.
For details: https://www.ruby-lang.org/bugreport.html

Aborted
```

Related issues:

Has duplicate Ruby trunk - Bug #15248: Segfault/memory corruption in vm.c:1946	**Closed**

Associated revisions

Revision 71b0d20f - 10/24/2018 10:38 AM - nobu (Nobuyoshi Nakada)

compile.c: fix peephole optimization

- compile.c (iseq_peephole_optimize): should pop before jump instruction which succeeds to newarray of a literal object, not after. [ruby-core:89536] [Bug #15245]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@65350 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 65350 - 10/24/2018 10:38 AM - nobu (Nobuyoshi Nakada)

compile.c: fix peephole optimization

- compile.c (iseq_peephole_optimize): should pop before jump instruction which succeeds to newarray of a literal object, not after. [ruby-core:89536] [Bug #15245]

Revision 65350 - 10/24/2018 10:38 AM - nobu (Nobuyoshi Nakada)

compile.c: fix peephole optimization

- compile.c (iseq_peephole_optimize): should pop before jump instruction which succeeds to newarray of a literal object, not after. [ruby-core:89536] [Bug #15245]

Revision 75600918 - 11/06/2018 03:13 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 65350: [Backport #15245]

```
    compile.c: fix peephole optimization

    * compile.c (iseq_peephole_optimize): should `pop` before jump
      instruction which succeeds to `newarray` of a literal object,
      not after.  [ruby-core:89536] [Bug #15245]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_5@65580 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 65580 - 11/06/2018 03:13 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 65350: [Backport #15245]

```
compile.c: fix peephole optimization

* compile.c (iseq_peephole_optimize): should `pop` before jump
  instruction which succeeds to `newarray` of a literal object,
  not after.  [ruby-core:89536] [Bug #15245]
```

History

#1 - 10/23/2018 11:49 PM - wanabe (_ wanabe)

It may be due to peephole_optimization.

I went into an infinite loop without peephole_optimization.
It is an expected behaviour.

```
$ ruby -ve 'iseq = RubyVM::InstructionSequence.compile("%w(1) || 2 while 3", peephole_optimization: false); pu
ts iseq.disasm; iseq.eval'
ruby 2.6.0dev (2018-10-24 trunk 65341) [x86_64-linux]
<compiled>:1: warning: literal in condition
== disasm: #<ISeq:<compiled>@<compiled>:1 (1,0)-(1,18)> (catch: FALSE)
== catch table
| catch type: break  st: 0006 ed: 0015 sp: 0000 cont: 0015
| catch type: next   st: 0006 ed: 0015 sp: 0000 cont: 0003
| catch type: redo   st: 0006 ed: 0015 sp: 0000 cont: 0006
|------------------------------------------------------------------------
0000 jump                           12                              (   1)[Li]
0002 putnil
0003 pop
0004 jump                           12
0006 putstring                      "1"
0008 newarray                       1
0010 branchif                       12
0012 jump                           6
0014 putnil
0015 leave
^CTraceback (most recent call last):
    2: from -e:1:in `<main>'
    1: from -e:1:in `eval'
<compiled>:1:in `<compiled>': Interrupt
```

And I got SEGV with peephole_optimization.

```
$ ruby -ve 'iseq = RubyVM::InstructionSequence.compile("%w(1) || 2 while 3", peephole_optimization: true); put
s iseq.disasm; iseq.eval'
ruby 2.6.0dev (2018-10-24 trunk 65341) [x86_64-linux]
<compiled>:1: warning: literal in condition
== disasm: #<ISeq:<compiled>@<compiled>:1 (1,0)-(1,18)> (catch: FALSE)
== catch table
| catch type: break  st: 0004 ed: 0009 sp: 0000 cont: 0009
| catch type: next   st: 0004 ed: 0009 sp: 0000 cont: 0003
| catch type: redo   st: 0004 ed: 0009 sp: 0000 cont: 0004
|------------------------------------------------------------------------
0000 jump                           4                               (   1)[Li]
0002 putnil
0003 pop
0004 putstring                      "1"
0006 jump                           4
0008 putnil
0009 leave
<compiled>:1: [BUG] Segmentation fault at 0x000055d6d4924000
ruby 2.6.0dev (2018-10-24 trunk 65341) [x86_64-linux]

-- Control frame information -----------------------------------------------
c:0004 p:0004 s:-5775390691329 e:000013 TOP    <compiled>:1 [FINISH]
c:0003 p:---- s:0011 e:000010 CFUNC  :eval
c:0002 p:0033 s:0007 E:002428 EVAL   -e:1 [FINISH]
c:0001 p:0000 s:0003 E:000dd0 (none) [FINISH]

-- Ruby level backtrace information ----------------------------------------
-e:1:in `<main>'
-e:1:in `eval'
<compiled>:1:in `<compiled>'

-- Machine register context ------------------------------------------------
 RIP: 0x000055d6d307dd52 RBP: 0xfffffffffffffffc RSP: 0x00007ffcda768900
 RAX: 0x000055d6d3fa3b38 RBX: 0x000055d6d439f600 RCX: 0x000055d6d4924000
```

```
 RDX: 0x000055d6d3fa3b38 RDI: 0x000055d6d3fa3b38 RSI: 0x000055d6d4924008
  R8: 0x0000000000003f98  R9: 0x000055d6d3f49140 R10: 0x0000000000000b58
 R11: 0x000000000000016c R12: 0x00007fdc5584bfa0 R13: 0x000055d6d404e530
 R14: 0x000055d6d439f600 R15: 0x00007fdc5584bf30 EFL: 0x0000000000010202

-- C level backtrace information -------------------------------------------
malloc_consolidate(): invalid chunk size
```

#2 - 10/24/2018 09:54 AM - nobu (Nobuyoshi Nakada)

- Has duplicate Bug #15248: Segfault/memory corruption in vm.c:1946 added

#3 - 10/24/2018 10:38 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

Applied in changeset trunk|r65350.

---

compile.c: fix peephole optimization

- compile.c (iseq_peephole_optimize): should pop before jump instruction which succeeds to newarray of a literal object, not after. [ruby-core:89536] [Bug #15245]

#4 - 10/24/2018 11:48 AM - nagachika (Tomoyuki Chikanaga)

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

I think r59892 introduce this bug. I'll fill Backport field according to the changeset timing. I didn't confirm it's actually reprodusible on stable branches.

#5 - 10/24/2018 12:02 PM - nobu (Nobuyoshi Nakada)

Yes, 2.4 is ok but 2.5 crashes.

```
$ ruby2.4 -v -e 'i = 0; %w(1) || 2 while (i += 1) < 100; p i'
ruby 2.4.5p335 (2018-10-18 revision 65137) [x86_64-darwin18]
100

$ ruby2.5 -v -e 'i = 0; %w(1) || 2 while (i += 1) < 100; p i'
ruby 2.5.3p105 (2018-10-18 revision 65156) [x86_64-darwin18]
100
-e:1: [BUG] Stack consistency error (sp: 106, bp: 7)
```

#6 - 11/06/2018 03:13 PM - nagachika (Tomoyuki Chikanaga)

- 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 r65580 merged revision(s) 65350.