Ruby master - Bug #15793

Please backport 7b7043e5da8589e01b94575d4ed647e909e5c875

04/26/2019 07:19 AM - shyouhei (Shyouhei Urabe)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:		**Backport:**	2.4: REQUIRED, 2.5: DONE, 2.6: DONE

Description

7b7043e5da8589e01b94575d4ed647e909e5c875 is a fix of use-after-free. Worth backporting methinks.

Associated revisions

Revision f4fe2a76 - 06/13/2019 12:23 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 7b7043e5da8589e01b94575d4ed647e909e5c875: [Backport #15793]

```
    eliminate use of freed memory

    rb_io_fptr_finalize_internal frees the memory region.

    =================================================================
    ==85264==ERROR: AddressSanitizer: heap-use-after-free on address 0x610000000d8c at pc 0x5608e38077f7 bp 0x
7ffee12d5440 sp 0x7ffee12d5438
    READ of size 4 at 0x610000000d8c thread T0
        #0 0x5608e38077f6 in rb_io_memsize io.c:4749:24
        #1 0x5608e37a0481 in obj_memsize_of gc.c:3547:14
        #2 0x5608e37a4f30 in check_rvalue_consistency gc.c:1107:2
        #3 0x5608e37a2624 in RVALUE_OLD_P gc.c:1218:5
        #4 0x5608e37a5bae in rb_gc_force_recycle gc.c:6652:18
        #5 0x5608e38191f9 in rb_f_backquote io.c:9021:5
        #6 0x5608e3d8aa14 in call_cfunc_1 vm_insnhelper.c:2058:12
        #7 0x5608e3d6e23d in vm_call_cfunc_with_frame vm_insnhelper.c:2211:11
        #8 0x5608e3d54a35 in vm_call_cfunc vm_insnhelper.c:2229:12
        #9 0x5608e3d5253b in vm_call_method_each_type vm_insnhelper.c:2564:9
        #10 0x5608e3d51f50 in vm_call_method vm_insnhelper.c:2701:13
        #11 0x5608e3cf2de4 in vm_call_general vm_insnhelper.c:2734:12
        #12 0x5608e3d79918 in vm_sendish vm_insnhelper.c:3627:11
        #13 0x5608e3d06cf5 in vm_exec_core insns.def:789:11
        #14 0x5608e3d43700 in rb_vm_exec vm.c:1892:22
        #15 0x5608e3d47cbf in rb_iseq_eval_main vm.c:2151:11
        #16 0x5608e37620ca in ruby_exec_internal eval.c:262:2
        #17 0x5608e376198b in ruby_exec_node eval.c:326:12
        #18 0x5608e37617d0 in ruby_run_node eval.c:318:25
        #19 0x5608e35c9486 in main main.c:42:9
        #20 0x7f62e9421b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
        #21 0x5608e3522289 in _start (miniruby+0x15f289)

    0x610000000d8c is located 76 bytes inside of 192-byte region [0x610000000d40,0x610000000e00)
    freed by thread T0 here:
        #0 0x5608e359a2ed in free (miniruby+0x1d72ed)
        #1 0x5608e37af421 in objspace_xfree gc.c:9591:5
        #2 0x5608e37af3da in ruby_sized_xfree gc.c:9687:2
        #3 0x5608e3799ac8 in ruby_xfree gc.c:9694:5
        #4 0x5608e380746d in rb_io_fptr_finalize_internal io.c:4728:5
        #5 0x5608e38191ed in rb_f_backquote io.c:9020:5
        #6 0x5608e3d8aa14 in call_cfunc_1 vm_insnhelper.c:2058:12
        #7 0x5608e3d6e23d in vm_call_cfunc_with_frame vm_insnhelper.c:2211:11
        #8 0x5608e3d54a35 in vm_call_cfunc vm_insnhelper.c:2229:12
        #9 0x5608e3d5253b in vm_call_method_each_type vm_insnhelper.c:2564:9
        #10 0x5608e3d51f50 in vm_call_method vm_insnhelper.c:2701:13
        #11 0x5608e3cf2de4 in vm_call_general vm_insnhelper.c:2734:12
        #12 0x5608e3d79918 in vm_sendish vm_insnhelper.c:3627:11
        #13 0x5608e3d06cf5 in vm_exec_core insns.def:789:11
        #14 0x5608e3d43700 in rb_vm_exec vm.c:1892:22
        #15 0x5608e3d47cbf in rb_iseq_eval_main vm.c:2151:11
        #16 0x5608e37620ca in ruby_exec_internal eval.c:262:2
        #17 0x5608e376198b in ruby_exec_node eval.c:326:12
```

```
        #18 0x5608e37617d0 in ruby_run_node eval.c:318:25
        #19 0x5608e35c9486 in main main.c:42:9
        #20 0x7f62e9421b96 in __libc_start_main
    /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

    previously allocated by thread T0 here:
        #0 0x5608e359a56d in malloc (miniruby+0x1d756d)
        #1 0x5608e37aed12 in objspace_xmalloc0 gc.c:9416:5
        #2 0x5608e37aebe7 in ruby_xmalloc0 gc.c:9600:12
        #3 0x5608e37aea8b in ruby_xmalloc_body gc.c:9609:12
        #4 0x5608e37a6d64 in ruby_xmalloc gc.c:11469:12
        #5 0x5608e380e4b4 in rb_io_fptr_new io.c:8040:19
        #6 0x5608e380e446 in rb_io_make_open_file io.c:8077:10
        #7 0x5608e3850ea0 in pipe_open io.c:6707:5
        #8 0x5608e384edb4 in pipe_open_s io.c:6772:12
        #9 0x5608e381910b in rb_f_backquote io.c:9014:12
        #10 0x5608e3d8aa14 in call_cfunc_1 vm_insnhelper.c:2058:12
        #11 0x5608e3d6e23d in vm_call_cfunc_with_frame vm_insnhelper.c:2211:11
        #12 0x5608e3d54a35 in vm_call_cfunc vm_insnhelper.c:2229:12
        #13 0x5608e3d5253b in vm_call_method_each_type vm_insnhelper.c:2564:9
        #14 0x5608e3d51f50 in vm_call_method vm_insnhelper.c:2701:13
        #15 0x5608e3cf2de4 in vm_call_general vm_insnhelper.c:2734:12
        #16 0x5608e3d79918 in vm_sendish vm_insnhelper.c:3627:11
        #17 0x5608e3d06cf5 in vm_exec_core insns.def:789:11
        #18 0x5608e3d43700 in rb_vm_exec vm.c:1892:22
        #19 0x5608e3d47cbf in rb_iseq_eval_main vm.c:2151:11
        #20 0x5608e37620ca in ruby_exec_internal eval.c:262:2
        #21 0x5608e376198b in ruby_exec_node eval.c:326:12
        #22 0x5608e37617d0 in ruby_run_node eval.c:318:25
        #23 0x5608e35c9486 in main main.c:42:9
        #24 0x7f62e9421b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

    SUMMARY: AddressSanitizer: heap-use-after-free io.c:4749:24 in
    rb_io_memsize
    Shadow bytes around the buggy address:
      0x0c207fff8160: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
      0x0c207fff8170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      0x0c207fff8180: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
      0x0c207fff8190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      0x0c207fff81a0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
    =>0x0c207fff81b0: fd[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd fd
      0x0c207fff81c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
      0x0c207fff81d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
      0x0c207fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
      0x0c207fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
      0x0c207fff8200: 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
      Shadow gap:              cc
    ==85264==ABORTING
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67710 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 67710 - 06/13/2019 12:23 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 7b7043e5da8589e01b94575d4ed647e909e5c875: [Backport #15793]

```
eliminate use of freed memory
```

```
rb_io_fptr_finalize_internal frees the memory region.

=================================================================
==85264==ERROR: AddressSanitizer: heap-use-after-free on address 0x610000000d8c at pc 0x5608e38077f7 bp 0x7ffe
e12d5440 sp 0x7ffee12d5438
READ of size 4 at 0x610000000d8c thread T0
    #0 0x5608e38077f6 in rb_io_memsize io.c:4749:24
    #1 0x5608e37a0481 in obj_memsize_of gc.c:3547:14
    #2 0x5608e37a4f30 in check_rvalue_consistency gc.c:1107:2
    #3 0x5608e37a2624 in RVALUE_OLD_P gc.c:1218:5
    #4 0x5608e37a5bae in rb_gc_force_recycle gc.c:6652:18
    #5 0x5608e38191f9 in rb_f_backquote io.c:9021:5
    #6 0x5608e3d8aa14 in call_cfunc_1 vm_insnhelper.c:2058:12
    #7 0x5608e3d6e23d in vm_call_cfunc_with_frame vm_insnhelper.c:2211:11
    #8 0x5608e3d54a35 in vm_call_cfunc vm_insnhelper.c:2229:12
    #9 0x5608e3d5253b in vm_call_method_each_type vm_insnhelper.c:2564:9
    #10 0x5608e3d51f50 in vm_call_method vm_insnhelper.c:2701:13
    #11 0x5608e3cf2de4 in vm_call_general vm_insnhelper.c:2734:12
    #12 0x5608e3d79918 in vm_sendish vm_insnhelper.c:3627:11
    #13 0x5608e3d06cf5 in vm_exec_core insns.def:789:11
    #14 0x5608e3d43700 in rb_vm_exec vm.c:1892:22
    #15 0x5608e3d47cbf in rb_iseq_eval_main vm.c:2151:11
    #16 0x5608e37620ca in ruby_exec_internal eval.c:262:2
    #17 0x5608e376198b in ruby_exec_node eval.c:326:12
    #18 0x5608e37617d0 in ruby_run_node eval.c:318:25
    #19 0x5608e35c9486 in main main.c:42:9
    #20 0x7f62e9421b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
    #21 0x5608e3522289 in _start (miniruby+0x15f289)

0x610000000d8c is located 76 bytes inside of 192-byte region [0x610000000d40,0x610000000e00)
freed by thread T0 here:
    #0 0x5608e359a2ed in free (miniruby+0x1d72ed)
    #1 0x5608e37af421 in objspace_xfree gc.c:9591:5
    #2 0x5608e37af3da in ruby_sized_xfree gc.c:9687:2
    #3 0x5608e3799ac8 in ruby_xfree gc.c:9694:5
    #4 0x5608e380746d in rb_io_fptr_finalize_internal io.c:4728:5
    #5 0x5608e38191ed in rb_f_backquote io.c:9020:5
    #6 0x5608e3d8aa14 in call_cfunc_1 vm_insnhelper.c:2058:12
    #7 0x5608e3d6e23d in vm_call_cfunc_with_frame vm_insnhelper.c:2211:11
    #8 0x5608e3d54a35 in vm_call_cfunc vm_insnhelper.c:2229:12
    #9 0x5608e3d5253b in vm_call_method_each_type vm_insnhelper.c:2564:9
    #10 0x5608e3d51f50 in vm_call_method vm_insnhelper.c:2701:13
    #11 0x5608e3cf2de4 in vm_call_general vm_insnhelper.c:2734:12
    #12 0x5608e3d79918 in vm_sendish vm_insnhelper.c:3627:11
    #13 0x5608e3d06cf5 in vm_exec_core insns.def:789:11
    #14 0x5608e3d43700 in rb_vm_exec vm.c:1892:22
    #15 0x5608e3d47cbf in rb_iseq_eval_main vm.c:2151:11
    #16 0x5608e37620ca in ruby_exec_internal eval.c:262:2
    #17 0x5608e376198b in ruby_exec_node eval.c:326:12
    #18 0x5608e37617d0 in ruby_run_node eval.c:318:25
    #19 0x5608e35c9486 in main main.c:42:9
    #20 0x7f62e9421b96 in __libc_start_main
/build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

previously allocated by thread T0 here:
    #0 0x5608e359a56d in malloc (miniruby+0x1d756d)
    #1 0x5608e37aed12 in objspace_xmalloc0 gc.c:9416:5
    #2 0x5608e37aebe7 in ruby_xmalloc0 gc.c:9600:12
    #3 0x5608e37aea8b in ruby_xmalloc_body gc.c:9609:12
    #4 0x5608e37a6d64 in ruby_xmalloc gc.c:11469:12
    #5 0x5608e380e4b4 in rb_io_fptr_new io.c:8040:19
    #6 0x5608e380e446 in rb_io_make_open_file io.c:8077:10
    #7 0x5608e3850ea0 in pipe_open io.c:6707:5
    #8 0x5608e384edb4 in pipe_open_s io.c:6772:12
    #9 0x5608e381910b in rb_f_backquote io.c:9014:12
    #10 0x5608e3d8aa14 in call_cfunc_1 vm_insnhelper.c:2058:12
    #11 0x5608e3d6e23d in vm_call_cfunc_with_frame vm_insnhelper.c:2211:11
    #12 0x5608e3d54a35 in vm_call_cfunc vm_insnhelper.c:2229:12
    #13 0x5608e3d5253b in vm_call_method_each_type vm_insnhelper.c:2564:9
    #14 0x5608e3d51f50 in vm_call_method vm_insnhelper.c:2701:13
    #15 0x5608e3cf2de4 in vm_call_general vm_insnhelper.c:2734:12
    #16 0x5608e3d79918 in vm_sendish vm_insnhelper.c:3627:11
    #17 0x5608e3d06cf5 in vm_exec_core insns.def:789:11
    #18 0x5608e3d43700 in rb_vm_exec vm.c:1892:22
```

```
    #19 0x5608e3d47cbf in rb_iseq_eval_main vm.c:2151:11
    #20 0x5608e37620ca in ruby_exec_internal eval.c:262:2
    #21 0x5608e376198b in ruby_exec_node eval.c:326:12
    #22 0x5608e37617d0 in ruby_run_node eval.c:318:25
    #23 0x5608e35c9486 in main main.c:42:9
    #24 0x7f62e9421b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: heap-use-after-free io.c:4749:24 in
rb_io_memsize
Shadow bytes around the buggy address:
  0x0c207fff8160: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c207fff8170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff8180: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c207fff8190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff81a0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
=>0x0c207fff81b0: fd[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c207fff81c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff81d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8200: 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
  Shadow gap:              cc
==85264==ABORTING
```

Revision bad64833 - 08/19/2019 06:35 AM - usa (Usaku NAKAMURA)

merge revision(s) f4fe2a76b0564e8e572936dec3bd724ac22b7a44: [Backport #15793]

```
    merge revision(s) 7b7043e5da8589e01b94575d4ed647e909e5c875: [Backport
     #15793]

            eliminate use of freed memory

            rb_io_fptr_finalize_internal frees the memory region.

            ==================================================================
            ==85264==ERROR: AddressSanitizer: heap-use-after-free on address 0x610000000d8c at pc 0x5608e38077
f7 bp 0x7ffee12d5440 sp 0x7ffee12d5438
            READ of size 4 at 0x610000000d8c thread T0
                #0 0x5608e38077f6 in rb_io_memsize io.c:4749:24
                #1 0x5608e37a0481 in obj_memsize_of gc.c:3547:14
                #2 0x5608e37a4f30 in check_rvalue_consistency gc.c:1107:2
                #3 0x5608e37a2624 in RVALUE_OLD_P gc.c:1218:5
                #4 0x5608e37a5bae in rb_gc_force_recycle gc.c:6652:18
                #5 0x5608e38191f9 in rb_f_backquote io.c:9021:5
                #6 0x5608e3d8aa14 in call_cfunc_1 vm_insnhelper.c:2058:12
                #7 0x5608e3d6e23d in vm_call_cfunc_with_frame vm_insnhelper.c:2211:11
                #8 0x5608e3d54a35 in vm_call_cfunc vm_insnhelper.c:2229:12
                #9 0x5608e3d5253b in vm_call_method_each_type vm_insnhelper.c:2564:9
                #10 0x5608e3d51f50 in vm_call_method vm_insnhelper.c:2701:13
                #11 0x5608e3cf2de4 in vm_call_general vm_insnhelper.c:2734:12
                #12 0x5608e3d79918 in vm_sendish vm_insnhelper.c:3627:11
                #13 0x5608e3d06cf5 in vm_exec_core insns.def:789:11
                #14 0x5608e3d43700 in rb_vm_exec vm.c:1892:22
                #15 0x5608e3d47cbf in rb_iseq_eval_main vm.c:2151:11
                #16 0x5608e37620ca in ruby_exec_internal eval.c:262:2
```

```
    #17 0x5608e376198b in ruby_exec_node eval.c:326:12
    #18 0x5608e37617d0 in ruby_run_node eval.c:318:25
    #19 0x5608e35c9486 in main main.c:42:9
    #20 0x7f62e9421b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c
:310
    #21 0x5608e3522289 in _start (miniruby+0x15f289)

0x610000000d8c is located 76 bytes inside of 192-byte region [0x610000000d40,0x610000000e00)
freed by thread T0 here:
    #0 0x5608e359a2ed in free (miniruby+0x1d72ed)
    #1 0x5608e37af421 in objspace_xfree gc.c:9591:5
    #2 0x5608e37af3da in ruby_sized_xfree gc.c:9687:2
    #3 0x5608e3799ac8 in ruby_xfree gc.c:9694:5
    #4 0x5608e380746d in rb_io_fptr_finalize_internal io.c:4728:5
    #5 0x5608e38191ed in rb_f_backquote io.c:9020:5
    #6 0x5608e3d8aa14 in call_cfunc_1 vm_insnhelper.c:2058:12
    #7 0x5608e3d6e23d in vm_call_cfunc_with_frame vm_insnhelper.c:2211:11
    #8 0x5608e3d54a35 in vm_call_cfunc vm_insnhelper.c:2229:12
    #9 0x5608e3d5253b in vm_call_method_each_type vm_insnhelper.c:2564:9
    #10 0x5608e3d51f50 in vm_call_method vm_insnhelper.c:2701:13
    #11 0x5608e3cf2de4 in vm_call_general vm_insnhelper.c:2734:12
    #12 0x5608e3d79918 in vm_sendish vm_insnhelper.c:3627:11
    #13 0x5608e3d06cf5 in vm_exec_core insns.def:789:11
    #14 0x5608e3d43700 in rb_vm_exec vm.c:1892:22
    #15 0x5608e3d47cbf in rb_iseq_eval_main vm.c:2151:11
    #16 0x5608e37620ca in ruby_exec_internal eval.c:262:2
    #17 0x5608e376198b in ruby_exec_node eval.c:326:12
    #18 0x5608e37617d0 in ruby_run_node eval.c:318:25
    #19 0x5608e35c9486 in main main.c:42:9
    #20 0x7f62e9421b96 in __libc_start_main
/build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

previously allocated by thread T0 here:
    #0 0x5608e359a56d in malloc (miniruby+0x1d756d)
    #1 0x5608e37aed12 in objspace_xmalloc0 gc.c:9416:5
    #2 0x5608e37aebe7 in ruby_xmalloc0 gc.c:9600:12
    #3 0x5608e37aea8b in ruby_xmalloc_body gc.c:9609:12
    #4 0x5608e37a6d64 in ruby_xmalloc gc.c:11469:12
    #5 0x5608e380e4b4 in rb_io_fptr_new io.c:8040:19
    #6 0x5608e380e446 in rb_io_make_open_file io.c:8077:10
    #7 0x5608e3850ea0 in pipe_open io.c:6707:5
    #8 0x5608e384edb4 in pipe_open_s io.c:6772:12
    #9 0x5608e381910b in rb_f_backquote io.c:9014:12
    #10 0x5608e3d8aa14 in call_cfunc_1 vm_insnhelper.c:2058:12
    #11 0x5608e3d6e23d in vm_call_cfunc_with_frame vm_insnhelper.c:2211:11
    #12 0x5608e3d54a35 in vm_call_cfunc vm_insnhelper.c:2229:12
    #13 0x5608e3d5253b in vm_call_method_each_type vm_insnhelper.c:2564:9
    #14 0x5608e3d51f50 in vm_call_method vm_insnhelper.c:2701:13
    #15 0x5608e3cf2de4 in vm_call_general vm_insnhelper.c:2734:12
    #16 0x5608e3d79918 in vm_sendish vm_insnhelper.c:3627:11
    #17 0x5608e3d06cf5 in vm_exec_core insns.def:789:11
    #18 0x5608e3d43700 in rb_vm_exec vm.c:1892:22
    #19 0x5608e3d47cbf in rb_iseq_eval_main vm.c:2151:11
    #20 0x5608e37620ca in ruby_exec_internal eval.c:262:2
    #21 0x5608e376198b in ruby_exec_node eval.c:326:12
    #22 0x5608e37617d0 in ruby_run_node eval.c:318:25
    #23 0x5608e35c9486 in main main.c:42:9
    #24 0x7f62e9421b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c
:310

SUMMARY: AddressSanitizer: heap-use-after-free io.c:4749:24 in
rb_io_memsize
Shadow bytes around the buggy address:
  0x0c207fff8160: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c207fff8170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff8180: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c207fff8190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff81a0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
=>0x0c207fff81b0: fd[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c207fff81c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff81d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8200: 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
            Shadow gap:              cc
          ==85264==ABORTING
```

```
    git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67710 b2dd03c8-39d4-4d8f-98ff-823fe69b080e
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_5@67748 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 67748 - 08/19/2019 06:35 AM - usa (Usaku NAKAMURA)

merge revision(s) f4fe2a76b0564e8e572936dec3bd724ac22b7a44: [Backport #15793]

```
merge revision(s) 7b7043e5da8589e01b94575d4ed647e909e5c875: [Backport
 #15793]

    eliminate use of freed memory

    rb_io_fptr_finalize_internal frees the memory region.

    =================================================================
    ==85264==ERROR: AddressSanitizer: heap-use-after-free on address 0x610000000d8c at pc 0x5608e38077f7 bp 0x
7ffee12d5440 sp 0x7ffee12d5438
    READ of size 4 at 0x610000000d8c thread T0
        #0 0x5608e38077f6 in rb_io_memsize io.c:4749:24
        #1 0x5608e37a0481 in obj_memsize_of gc.c:3547:14
        #2 0x5608e37a4f30 in check_rvalue_consistency gc.c:1107:2
        #3 0x5608e37a2624 in RVALUE_OLD_P gc.c:1218:5
        #4 0x5608e37a5bae in rb_gc_force_recycle gc.c:6652:18
        #5 0x5608e38191f9 in rb_f_backquote io.c:9021:5
        #6 0x5608e3d8aa14 in call_cfunc_1 vm_insnhelper.c:2058:12
        #7 0x5608e3d6e23d in vm_call_cfunc_with_frame vm_insnhelper.c:2211:11
        #8 0x5608e3d54a35 in vm_call_cfunc vm_insnhelper.c:2229:12
        #9 0x5608e3d5253b in vm_call_method_each_type vm_insnhelper.c:2564:9
        #10 0x5608e3d51f50 in vm_call_method vm_insnhelper.c:2701:13
        #11 0x5608e3cf2de4 in vm_call_general vm_insnhelper.c:2734:12
        #12 0x5608e3d79918 in vm_sendish vm_insnhelper.c:3627:11
        #13 0x5608e3d06cf5 in vm_exec_core insns.def:789:11
        #14 0x5608e3d43700 in rb_vm_exec vm.c:1892:22
        #15 0x5608e3d47cbf in rb_iseq_eval_main vm.c:2151:11
        #16 0x5608e37620ca in ruby_exec_internal eval.c:262:2
        #17 0x5608e376198b in ruby_exec_node eval.c:326:12
        #18 0x5608e37617d0 in ruby_run_node eval.c:318:25
        #19 0x5608e35c9486 in main main.c:42:9
        #20 0x7f62e9421b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
        #21 0x5608e3522289 in _start (miniruby+0x15f289)

    0x610000000d8c is located 76 bytes inside of 192-byte region [0x610000000d40,0x610000000e00)
    freed by thread T0 here:
        #0 0x5608e359a2ed in free (miniruby+0x1d72ed)
        #1 0x5608e37af421 in objspace_xfree gc.c:9591:5
        #2 0x5608e37af3da in ruby_sized_xfree gc.c:9687:2
        #3 0x5608e3799ac8 in ruby_xfree gc.c:9694:5
        #4 0x5608e380746d in rb_io_fptr_finalize_internal io.c:4728:5
        #5 0x5608e38191ed in rb_f_backquote io.c:9020:5
        #6 0x5608e3d8aa14 in call_cfunc_1 vm_insnhelper.c:2058:12
        #7 0x5608e3d6e23d in vm_call_cfunc_with_frame vm_insnhelper.c:2211:11
        #8 0x5608e3d54a35 in vm_call_cfunc vm_insnhelper.c:2229:12
        #9 0x5608e3d5253b in vm_call_method_each_type vm_insnhelper.c:2564:9
```

```
    #10 0x5608e3d51f50 in vm_call_method vm_insnhelper.c:2701:13
    #11 0x5608e3cf2de4 in vm_call_general vm_insnhelper.c:2734:12
    #12 0x5608e3d79918 in vm_sendish vm_insnhelper.c:3627:11
    #13 0x5608e3d06cf5 in vm_exec_core insns.def:789:11
    #14 0x5608e3d43700 in rb_vm_exec vm.c:1892:22
    #15 0x5608e3d47cbf in rb_iseq_eval_main vm.c:2151:11
    #16 0x5608e37620ca in ruby_exec_internal eval.c:262:2
    #17 0x5608e376198b in ruby_exec_node eval.c:326:12
    #18 0x5608e37617d0 in ruby_run_node eval.c:318:25
    #19 0x5608e35c9486 in main main.c:42:9
    #20 0x7f62e9421b96 in __libc_start_main
/build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

previously allocated by thread T0 here:
    #0 0x5608e359a56d in malloc (miniruby+0x1d756d)
    #1 0x5608e37aed12 in objspace_xmalloc0 gc.c:9416:5
    #2 0x5608e37aebe7 in ruby_xmalloc0 gc.c:9600:12
    #3 0x5608e37aea8b in ruby_xmalloc_body gc.c:9609:12
    #4 0x5608e37a6d64 in ruby_xmalloc gc.c:11469:12
    #5 0x5608e380e4b4 in rb_io_fptr_new io.c:8040:19
    #6 0x5608e380e446 in rb_io_make_open_file io.c:8077:10
    #7 0x5608e3850ea0 in pipe_open io.c:6707:5
    #8 0x5608e384edb4 in pipe_open_s io.c:6772:12
    #9 0x5608e381910b in rb_f_backquote io.c:9014:12
    #10 0x5608e3d8aa14 in call_cfunc_1 vm_insnhelper.c:2058:12
    #11 0x5608e3d6e23d in vm_call_cfunc_with_frame vm_insnhelper.c:2211:11
    #12 0x5608e3d54a35 in vm_call_cfunc vm_insnhelper.c:2229:12
    #13 0x5608e3d5253b in vm_call_method_each_type vm_insnhelper.c:2564:9
    #14 0x5608e3d51f50 in vm_call_method vm_insnhelper.c:2701:13
    #15 0x5608e3cf2de4 in vm_call_general vm_insnhelper.c:2734:12
    #16 0x5608e3d79918 in vm_sendish vm_insnhelper.c:3627:11
    #17 0x5608e3d06cf5 in vm_exec_core insns.def:789:11
    #18 0x5608e3d43700 in rb_vm_exec vm.c:1892:22
    #19 0x5608e3d47cbf in rb_iseq_eval_main vm.c:2151:11
    #20 0x5608e37620ca in ruby_exec_internal eval.c:262:2
    #21 0x5608e376198b in ruby_exec_node eval.c:326:12
    #22 0x5608e37617d0 in ruby_run_node eval.c:318:25
    #23 0x5608e35c9486 in main main.c:42:9
    #24 0x7f62e9421b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: heap-use-after-free io.c:4749:24 in
rb_io_memsize
Shadow bytes around the buggy address:
  0x0c207fff8160: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c207fff8170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff8180: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c207fff8190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff81a0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
=>0x0c207fff81b0: fd[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c207fff81c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff81d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8200: 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
  Shadow gap:              cc
==85264==ABORTING
```

```
git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67710 b2dd03c8-39d4-4d8f-98ff-823fe69b080e
```

History

#1 - 04/26/2019 12:48 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.4: UNKNOWN, 2.5: UNKNOWN, 2.6: UNKNOWN to 2.4: REQUIRED, 2.5: REQUIRED, 2.6: REQUIRED

#2 - 06/13/2019 12:24 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.4: REQUIRED, 2.5: REQUIRED, 2.6: REQUIRED to 2.4: REQUIRED, 2.5: REQUIRED, 2.6: DONE

Backported into ruby_2_6 at r67710.

#3 - 08/19/2019 06:35 AM - usa (Usaku NAKAMURA)

- Backport changed from 2.4: REQUIRED, 2.5: REQUIRED, 2.6: DONE to 2.4: REQUIRED, 2.5: DONE, 2.6: DONE

ruby_2_5 r67748 merged revision(s) f4fe2a76b0564e8e572936dec3bd724ac22b7a44.