Out-of-bounds Read in mruby/mruby

Valid Reported on Feb 16th 2022

0

Description

commit ecb28f4bf463483cf914c799d086b0cfff997aee

Proof of Concept

```
 root@pocas   ~/fuzz/mruby2     master ±   echo "P2MKWyoqMCwqKjgsbTowXQS
 root@pocas   ~/fuzz/mruby2     master ±   ./bin/mruby poc1
AddressSanitizer:DEADLYSIGNAL
=================================================================
==2524121==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000011
==2524121==The signal is caused by a READ memory access.
==2524121==Hint: address points to the zero page.
    #0 0x59fd79 in mrb_check_frozen /root/fuzz/mruby2/include/mruby.h:1418:
    #1 0x59fd79 in hash_modify /root/fuzz/mruby2/src/hash.c:1154:3
    #2 0x59fd79 in mrb_hash_merge /root/fuzz/mruby2/src/hash.c:1734:3
    #3 0x4df12f in mrb_vm_exec /root/fuzz/mruby2/src/vm.c:2780:7
    #4 0x4d77de in mrb_vm_run /root/fuzz/mruby2/src/vm.c:1128:12
    #5 0x5e9602 in mrb_load_exec /root/fuzz/mruby2/mrbgems/mruby-compiler/c
    #6 0x5ea4f3 in mrb_load_detect_file_cxt /root/fuzz/mruby2/mrbgems/mruby
    #7 0x4cb88b in main /root/fuzz/mruby2/mrbgems/mruby-bin-mruby/tools/mru
    #8 0x7ff4daabd564 in __libc_start_main csu/../csu/libc-start.c:332:16
    #9 0x41d7ad in _start (/root/fuzz/mruby2/bin/mruby+0x41d7ad)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /root/fuzz/mruby2/include/mruby.h:1418:7 in
==2524121==ABORTING
```


Impact

This vulnerability is capable of...

CVE
CVE-2022-0630
(Published)

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

Severity
High (7.1)

Visibility
Public

Status
Fixed

Found by

Pocas
@p0cas
amateur

Fixed by

Yukihiro "Matz" Matsumoto
@matz
maintainer

This report was seen 421 times.

We are processing your report and will contact the **mruby** team within 24 hours. 9 months ago

Pocas modified the report 9 months ago

Yukihiro "Matz" Matsumoto validated this vulnerability 9 months ago

Pocas has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Pocas 9 months ago Researcher

When do you patch?

Yukihiro "Matz" Matsumoto marked this as fixed in 3.2 with commit ff3a5e 9 months ago

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

This vulnerability will not receive a CVE ✖

Pocas 9 months ago Researcher

Again, the patch above has nothing to do with this issue. Found after the patched commit.

Yukihiro 9 months ago Maintainer

Hmm. I cannot reproduce the problem after ff3a5ebed6ffbe3e70481531cfb969b497aa73ad
Can you show us additional information to reproduce the issue, please?

Pocas 9 months ago Researcher

Ah! patch commit is correct sorry

Sign in to join this conversation