Use-After-Free in function hash_new_from_values in mruby/mruby

0

Valid Reported on May 27th 2022

Description

Use-After-Free in function hash_new_from_values at vm.c:1167

mruby version

```
git log
commit ac79849fde3381e001c3274fbcdda20a5c9cb22b (HEAD -> master, origin/mas
Author: Yukihiro "Matz" Matsumoto <matz@ruby.or.jp>
Date:   Fri May 20 09:59:23 2022 +0900
```

Build

```
export CFLAGS="-g -O0 -lpthread -fsanitize=address"
export CXXFLAGS="-g -O0 -lpthread -fsanitize=address"
export LDFLAGS="-fsanitize=address"
make
```

POC

```
./mruby /mnt/share/max/fuzz/poc/mruby/poc_uaf_s.rb
=================================================================
==3269441==ERROR: AddressSanitizer: heap-use-after-free on address 0x619000
READ of size 8 at 0x619000000438 thread T0
    #0 0x5deb13 in hash_new_from_values /home/fuzz/fuzz/mru
    #1 0x57d9c1 in mrb_vm_exec /home/fuzz/fuzz/mruby/src/vm.c:1628:7
```

```
    #2 0x56c3bd in mrb_vm_run /home/fuzz/fuzz/mruby/src/vm.c:1138:12
    #3 0x5656c4 in mrb_top_run /home/fuzz/fuzz/mruby/src/vm.c:3061:12
    #4 0x6b0c05 in mrb_load_exec /home/fuzz/fuzz/mruby/mrbgems/mruby-compil

    #5 0x6b232f in mrb_load_detect_file_cxt /home/fuzz/fuzz/mruby/mrbgems/m
    #6 0x4cb27a in main /home/fuzz/fuzz/mruby/mrbgems/mruby-bin-mruby/tools
    #7 0x7ffff7c4c082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/c
    #8 0x41d78d in _start (/home/fuzz/fuzz/mruby/bin/mruby+0x41d78d)

0x619000000438 is located 952 bytes inside of 1024-byte region [0x619000000
freed by thread T0 here:
    #0 0x498d09 in realloc (/home/fuzz/fuzz/mruby/bin/mruby+0x498d09)
    #1 0x6430bd in mrb_default_allocf /home/fuzz/fuzz/mruby/src/state.c:69
    #2 0x5e60d3 in mrb_realloc_simple /home/fuzz/fuzz/mruby/src/gc.c:227:8
    #3 0x55b5cb in stack_extend_alloc /home/fuzz/fuzz/mruby/src/vm.c:181:27
    #4 0x55aeee in mrb_stack_extend /home/fuzz/fuzz/mruby/src/vm.c:201:5
    #5 0x5616c2 in mrb_stack_extend_adjust /home/fuzz/fuzz/mruby/src/vm.c:2
    #6 0x55fa7f in mrb_funcall_with_block /home/fuzz/fuzz/mruby/src/vm.c:53
    #7 0x55dd5d in mrb_funcall_argv /home/fuzz/fuzz/mruby/src/vm.c:584:10
    #8 0x55e4aa in mrb_funcall_id /home/fuzz/fuzz/mruby/src/vm.c:409:10
    #9 0x60251a in mrb_eql /home/fuzz/fuzz/mruby/src/object.c:642:10
    #10 0x74220e in obj_eql /home/fuzz/fuzz/mruby/src/hash.c:379:5
    #11 0x743ccb in ea_get_by_key /home/fuzz/fuzz/mruby/src/hash.c:456:3
    #12 0x742b10 in ar_set /home/fuzz/fuzz/mruby/src/hash.c:526:16
    #13 0x735888 in h_set /home/fuzz/fuzz/mruby/src/hash.c:1012:3
    #14 0x7346be in mrb_hash_set /home/fuzz/fuzz/mruby/src/hash.c:1245:3
    #15 0x5deb54 in hash_new_from_values /home/fuzz/fuzz/mruby/src/vm.c:116
    #16 0x57d9c1 in mrb_vm_exec /home/fuzz/fuzz/mruby/src/vm.c:1628:7
    #17 0x56c3bd in mrb_vm_run /home/fuzz/fuzz/mruby/src/vm.c:1138:12
    #18 0x5656c4 in mrb_top_run /home/fuzz/fuzz/mruby/src/vm.c:3061:12
    #19 0x6b0c05 in mrb_load_exec /home/fuzz/fuzz/mruby/mrbgems/mruby-compi
    #20 0x6b232f in mrb_load_detect_file_cxt /home/fuzz/fuzz/mruby/mrbgems/
    #21 0x4cb27a in main /home/fuzz/fuzz/mruby/mrbgems/mruby-bin-mruby/tool
    #22 0x7ffff7c4c082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

previously allocated by thread T0 here:
    #0 0x498d09 in realloc (/home/fuzz/fuzz/mruby/bin/mruby+0x498d09)
    #1 0x6430bd in mrb_default_allocf /home/fuzz/fuzz/mruby/src/state.c:69
    #2 0x5e60d3 in mrb_realloc_simple /home/fuzz/fuzz/mruby/
    #3 0x5e6999 in mrb_realloc /home/fuzz/fuzz/mruby/src/gc
    #4 0x5e6b81 in mrb_malloc /home/fuzz/fuzz/mruby/src/gc.c:257:10
```

```
    #5 0x5e6d62 in mrb_calloc /home/fuzz/fuzz/mruby/src/gc.c:275:9
    #6 0x560b03 in stack_init /home/fuzz/fuzz/mruby/src/vm.c:110:28
    #7 0x56c1a6 in mrb_vm_run /home/fuzz/fuzz/mruby/src/vm.c:1131:5

    #8 0x565499 in mrb_top_run /home/fuzz/fuzz/mruby/src/vm.c:3057:12
    #9 0x552360 in mrb_load_proc /home/fuzz/fuzz/mruby/src/load.c:716:10
    #10 0x7a46f7 in mrb_init_mrblib /home/fuzz/fuzz/mruby/build/host/mrblib
    #11 0x727785 in mrb_init_core /home/fuzz/fuzz/mruby/src/init.c:50:3
    #12 0x643213 in init_gc_and_core /home/fuzz/fuzz/mruby/src/state.c:35:3
    #13 0x6401c1 in mrb_core_init_protect /home/fuzz/fuzz/mruby/src/error.c
    #14 0x642f37 in mrb_open_core /home/fuzz/fuzz/mruby/src/state.c:53:7
    #15 0x6433fd in mrb_open_allocf /home/fuzz/fuzz/mruby/src/state.c:92:20
    #16 0x64339b in mrb_open /home/fuzz/fuzz/mruby/src/state.c:76:20
    #17 0x4c9cf8 in main /home/fuzz/fuzz/mruby/mrbgems/mruby-bin-mruby/tool
    #18 0x7ffff7c4c082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

SUMMARY: AddressSanitizer: heap-use-after-free /home/fuzz/fuzz/mruby/src/vm
Shadow bytes around the buggy address:
  0x0c327fff8030: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8040: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8050: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8060: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8070: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c327fff8080: fd fd fd fd fd fd fd[fd]fd fd fd fd fd fd fd fd
  0x0c327fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff80b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff80c0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff80d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
```

```
    Poisoned by user:        f7
    Container overflow:      fc
    Array cookie:            ac

    Intra object redzone:    bb
    ASan internal:           fe
    Left alloca redzone:     ca
    Right alloca redzone:    cb
    Shadow gap:              cc
  ==3269441==ABORTING
```

poc_uaf_s.rb

Impact

Referencing memory after it has been freed can cause a program to crash, use unexpected values, or execute code.

Occurrences

C vm.c L1167

CVE
CVE-2022-1934
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
Medium (5.1)

Registry
Other

Affected Version
*

Visibility
Public

Status

Fixed

Found by

TDHX ICS Security

@jieyongma

pro

Fixed by

Yukihiro "Matz" Matsumoto

@matz

maintainer

This report was seen 620 times.

We are processing your report and will contact the **mruby** team within 24 hours. 6 months ago

We have contacted a member of the **mruby** team and are waiting to hear back 6 months ago

Yukihiro "Matz" Matsumoto modified the Severity from Critical (9.4) to Medium (5.1) 6 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

Yukihiro "Matz" Matsumoto validated this vulnerability 6 months ago

TDHX ICS Security has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Yukihiro "Matz" Matsumoto marked this as fixed in **3.2** with commit **aa7f98** 6 months ago

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

This vulnerability will not receive a CVE ×

vm.c#L1167 has been validated ✓

Yukihiro "Matz" Matsumoto gave praise 6 months ago

Thank you for the report. I modified severity according to our security policy.

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

Sign in to join this conversation