

[New issue](#)[Jump to bottom](#)

Null pointer dereference in qemu_ram_free when HVA malloc fails #1588

🔒 Closed liyansong2018 opened this issue on Apr 12 · 2 comments

liyansong2018 commented on Apr 12 • edited ▾

Contributor

When we try to use `uc_mem_map` to apply for super large memory, memory allocation in HAV fails, but succeeds in GVA. This inconsistency leads to null pointer dereference in `uc_close` release about the ram block requested by `uc_mem_map`.

PoC

```
int main(int argc, char **argv) {
    uc_engine *uc;
    uc_err err;
    err = uc_open(UC_ARCH_X86, UC_MODE_64, &uc);
    if (err != UC_ERR_OK) {
        printf("Failed on uc_open() with error returned: %u %s\n", err, uc_strerror(err));
        return -1;
    }

    err = uc_mem_map(uc, 0x0, 0xffffffff000, UC_PROT_ALL);
    if (err != UC_ERR_OK) {
        printf("Failed on uc_open() with error returned: %u %s\n", err, uc_strerror(err));
        //return -1;
    }
    uc_close(uc);
    return 0;
}
```

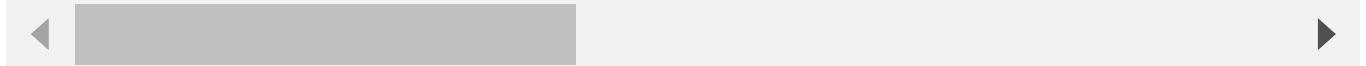
output



```
$ ./poc_test
AddressSanitizer:DEADLYSIGNAL
=====
==36945==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f6f0c61dc5f bp 0x7ffd
==36945==The signal is caused by a WRITE memory access.
==36945==Hint: address points to the zero page.
```

```
#0 0x7f6f0c61dc5f in qemu_ram_free_x86_64 /home/lys/Documents/my/unicorn/qemu/exec.c:1133
#1 0x7f6f0c624483 in memory_region_destructor_ram /home/lys/Documents/my/unicorn/qemu/softmmu/mem
#2 0x7f6f0c62269f in memory_free_x86_64 /home/lys/Documents/my/unicorn/qemu/softmmu/memory.c:182
#3 0x7f6f0c6169da in release_common /home/lys/Documents/my/unicorn/qemu/unicorn_common.h:62
#4 0x7f6f0c616cd3 in x86_release /home/lys/Documents/my/unicorn/qemu/target/i386/unicorn.c:47
#5 0x7f6f0c60e4c5 in uc_close /home/lys/Documents/my/unicorn/uc.c:419
#6 0x55955d1423e1 in main /home/lys/Documents/unitest/poc_test.c:60
#7 0x7f6f0c0d47ec in __libc_start_main ../csu/libc-start.c:332
#8 0x55955d142129 in _start (/home/lys/Documents/unitest/poc_test+0x1129)
```

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV /home/lys/Documents/my/unicorn/qemu/exec.c:1133 in qemu_ram_free_x86_==36945==ABORTING



  **liyansong2018** changed the title ~~Null pointer dereference in qemu_ram_free when HVA malloc failed~~
Null pointer dereference in qemu_ram_free when HVA malloc fails on Apr 12

liyansong2018 commented on Apr 12 • edited ▾

Contributor

Author

There are many ways to fix this bug. I will pull request with a simple patch later.

  **liyansong2018** mentioned this issue on Apr 13


Fix unicorn-engine#1588 #1590 #1589

 Closed

wtdcode commented on Apr 16

Member

Fixed in [3d3deac](#)

 **wtdcode** closed this as completed on Apr 16

  **jba** mentioned this issue on Jun 2

x/vulndb: potential Go vuln in github.com/unicorn-engine/unicorn: CVE-2022-29694
[jba/nested-modules#337](#)

 Open



GoVulnBot mentioned this issue on Jun 2

x/vulndb: potential Go vuln in github.com/unicorn-engine/unicorn: CVE-2022-29694
golang/vulndb#472

✓ Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

