unicorn-engine / **unicorn** Public

Code Issues 45 Pull requests 7 Discussions Actions Projects ...

New issue

Jump to bottom

Memory leaks caused by incomplete unicorn engine initialization. #1595

Closed **liyansong2018** opened this issue on Apr 16 · 1 comment

liyansong2018 commented on Apr 16 Contributor

Unicorn 2 provide a new API (`uc_ctl`) that allows host to modify the architecture and mode of the CPU. However, this api doesn't determine whether the architecture and mode are supported by unicorn. Further more, Unicorn did not judge the result of engine initialization at the design stage.

In other words, if we use unexpected architecture or mode to initialize unicorn engine, unicorn will alloc memory during initialization that will not be released.

```
NICORN_EXPORT
uc_err uc_close(uc_engine *uc)
{
    int i;
    MemoryRegion *mr;

    if (!uc->init_done) {
        free(uc);
        return UC_ERR_OK;
    }

    // Cleanup internally.
    if (uc->release) {
        uc->release(uc->tcg_ctx);
    }

    // ...
    g_free(uc->l1_map);

    free(uc);

    return UC_ERR_OK;
}
```

Although `uc->init_done` is equal to zero, something is alloced in memory region such as `uc->l1_map` .

PoC

```
#define ADDRESS 0x2000
#define SIZE 0x1000
#define MODE 1111

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_ctl(uc, UC_CTL_CPU_MODEL, MODE);
    if (err != UC_ERR_OK) {
        printf("Failed on uc_ctl() with error returned: %u %s\n", err, uc_strerror(err));
        return -1;
    }

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

    uc_close(uc);
    return 0;
}
```

Debug info

```
$ ./poc_test
Failed on uc_mem_map() with error returned: 20 Insufficient resource (UC_ERR_RESOURCE)

=================================================================
==23530==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 65536 byte(s) in 1 object(s) allocated from:
    #0 0x7f0372854037 in __interceptor_calloc ../../../../src/libsanitizer/asan/asan_malloc_linux.cpp
    #1 0x7f037145bfbc in g_malloc0 /home/lys/Documents/my/unicorn/glib_compat/gmem.c:139
    #2 0x7f03714b6a6b in tcg_exec_init_x86_64 /home/lys/Documents/my/unicorn/qemu/accel/tcg/translate
    #3 0x7f03714584ba in machine_initialize /home/lys/Documents/my/unicorn/qemu/softmmu/vl.c:53
    #4 0x7f0371453f55 in uc_init /home/lys/Documents/my/unicorn/uc.c:214
    #5 0x7f03714556a9 in uc_mem_map /home/lys/Documents/my/unicorn/uc.c:1010
    #6 0x5606ff4f335e in main /home/lys/Documents/unitest/poc_test.c:30
    #7 0x7f0370f1a7ec in __libc_start_main ../csu/libc-start.c:332

Direct leak of 42504 byte(s) in 1 object(s) allocated from:
    #0 0x7f0372853e8f in __interceptor_malloc ../../../../src/libsanitizer/asan/asan_malloc_linux.cpp
    #1 0x7f037145bf4e in g_malloc /home/lys/Documents/my/unicorn/glib_compat/gmem.c:93
    #2 0x7f03714b69dc in tcg_exec_init_x86_64 /home/lys/Documents/my/unicorn/qemu/accel/tcg/translate
    #3 0x7f03714584ba in machine_initialize /home/lys/Documents/my/unicorn/qemu/softmmu/vl.c:53
    #4 0x7f0371453f55 in uc_init /home/lys/Documents/my/unicorn/uc.c:214
    #5 0x7f03714556a9 in uc_mem_map /home/lys/Documents/my/unicorn/uc.c:1010
    #6 0x5606ff4f335e in main /home/lys/Documents/unitest/poc_test.c:30
    #7 0x7f0370f1a7ec in __libc_start_main ../csu/libc-start.c:332

Direct leak of 160 byte(s) in 1 object(s) allocated from:
    #0 0x7f0372853e8f in __interceptor_malloc ../../../../src/libsanitizer/asan/asan_malloc_linux.cpp
    #1 0x7f037145bf4e in g_malloc /home/lys/Documents/my/unicorn/glib_compat/gmem.c:93
    #2 0x7f03714644d8 in memory_map_init /home/lys/Documents/my/unicorn/qemu/exec.c:1463
    #3 0x7f0371464dae in cpu_exec_init_all_x86_64 /home/lys/Documents/my/unicorn/qemu/exec.c:1754
    #4 0x7f037145848d in machine_initialize /home/lys/Documents/my/unicorn/qemu/softmmu/vl.c:48
    #5 0x7f0371453f55 in uc_init /home/lys/Documents/my/unicorn/uc.c:214
    #6 0x7f03714556a9 in uc_mem_map /home/lys/Documents/my/unicorn/uc.c:1010
    #7 0x5606ff4f335e in main /home/lys/Documents/unitest/poc_test.c:30
    #8 0x7f0370f1a7ec in __libc_start_main ../csu/libc-start.c:332

#...
SUMMARY: AddressSanitizer: 710422 byte(s) leaked in 27 allocation(s).
```

wtdcode commented on Apr 16 Member

Fixed in 5a79d78

wtdcode closed this as completed on Apr 16

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants