

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

# Memory leaks caused by unexpected architecture in unicorn dev branch #1586

✓ Closed

liyansong2018 opened this issue on Apr 11 · 1 comment

liyansong2018 commented on Apr 11 • edited ▼

Contributor

Hi :)

When we used unexpected architecture such as `0`, there was a memory leak in unicorn2.

PoC

```
int main(int argc, char **argv) {
    uc_engine *uc;
    uc_err err;

    /* Initialize emulator in X86-64bit mode */
    err = uc_open(0, UC_MODE_64, &uc);

    if (err == UC_ERR_OK) {
        printf("Failed on uc_open() with error returned: %u\n", err);
        printf("%s\n", uc_strerror(err));
        return -1;
    }

    if (err == UC_ERR_ARCH) {
        printf("Failed on uc_open() with error returned: %u\n", err);
        printf("%s\n", uc_strerror(err));
    }

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

If we don't use `uc_close(uc)`, there will be a memory leak.

```
$ ./poc_test
Failed on uc_open() with error returned: 2
```

Invalid/unsupported architecture (UC\_ERR\_ARCH)

=====

==22499==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 14720 byte(s) in 1 object(s) allocated from:

```
#0 0x7f2082fde037 in __interceptor_calloc ../../src/libsanitizer/asan/asan_malloc_linux.cpp
#1 0x7f2081bddfce in uc_open /home/lys/Documents/my/unicorn/uc.c:236
#2 0x563051f0b278 in main /home/lys/Documents/unitest/poc_test.c:17
#3 0x7f20816a47ec in __libc_start_main ../csu/libc-start.c:332
```

SUMMARY: AddressSanitizer: 14720 byte(s) leaked in 1 allocation(s).



If we use `uc_close(uc)`, there will be a segmentation fault!

```
$ ./poc_test
```

```
Failed on uc_open() with error returned: 2
```

```
Invalid/unsupported architecture (UC_ERR_ARCH)
```

```
AddressSanitizer:DEADLYSIGNAL
```

=====

```
==22535==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000075d (pc 0x7f5eb03ee46b bp 0x7ffe
```

```
==22535==The signal is caused by a READ memory access.
```

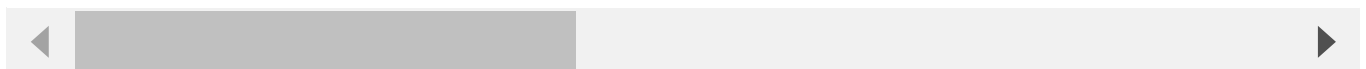
```
==22535==Hint: address points to the zero page.
```

```
#0 0x7f5eb03ee46b in uc_close /home/lys/Documents/my/unicorn/uc.c:412
#1 0x5573d73fb32d in main /home/lys/Documents/unitest/poc_test.c:30
#2 0x7f5eafeb47ec in __libc_start_main ../csu/libc-start.c:332
#3 0x5573d73fb119 in _start (/home/lys/Documents/unitest/poc_test+0x1119)
```

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV /home/lys/Documents/my/unicorn/uc.c:412 in uc\_close

```
==22535==ABORTING
```



 **wtdcode** added a commit that referenced this issue on Apr 11


 Merge pull request [#1587](#) from liyansong2018/dev ...

 469fc4c

**wtdcode** commented on Apr 11

Member

Closed due to PR merged.

 **wtdcode** closed this as completed on Apr 11

Assignees

No one assigned

---

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

2 participants

