

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

[BUG] two null pointer deference mujs-pp #161

✓ Closed kdsjZh opened this issue on May 13 · 0 comments

kdsjZh commented on May 13 • edited ▼

Brief summary

Hello, I was testing my fuzzer and found several bugs in mujs-pp.

Compiling the program

I compile mujs's latest commit [db110ea](#) in ubuntu 22 (docker image) with gcc 11.2.0-19ubuntu1.
With command `make build=sanitize`

BUG1

When parsing an incorrect argument (e.g. `./build/sanitize/mujs-pp -h`), a null pointer deference will be triggered. mujs-pp might didn't check the argument it parsed.

```
AddressSanitizer:DEADLYSIGNAL
=====
==1229272==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f182f7a1cfb bp
0x000000000000 sp 0x7fff2b38aa10 T0)
==1229272==The signal is caused by a READ memory access.
==1229272==Hint: address points to the zero page.
#0 0x7f182f7a1cfb in _IO_fclose (/lib/x86_64-linux-gnu/libc.so.6+0x82cfb)
#1 0x7f182fabee48 in __interceptor_fclose
../../../../src/libsanitizer/sanitizer_common/sanitizer_common_interceptors.inc:6233
#2 0x7f182fabee48 in __interceptor_fclose
../../../../src/libsanitizer/sanitizer_common/sanitizer_common_interceptors.inc:6228
#3 0x55c4ca90b44d in js_ppfile /benchmark/mujs/pp.c:37
#4 0x55c4ca90b985 in main /benchmark/mujs/pp.c:106
#5 0x7f182f74cd8f (/lib/x86_64-linux-gnu/libc.so.6+0x2dd8f)
#6 0x7f182f74ce3f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2de3f)
#7 0x55c4ca8a59c4 in _start (/benchmark/mujs/build/sanitize/mujs-pp+0x169c4)
```

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV (/lib/x86_64-linux-gnu/libc.so.6+0x82cfb) in _IO_fclose
==1229272==ABORTIN

BUG2

A null pointer dereference in jsP_dumpsyntax will be triggered when parsing a crafted js file, when running
./mujs-pp \$POC , as shown in the attachment

```
AddressSanitizer:DEADLYSIGNAL
=====
==1412001==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x55faed39dd7e bp
0x7ffe11e19bb0 sp 0x7ffe11e19b90 T0)
==1412001==The signal is caused by a READ memory access.
==1412001==Hint: address points to the zero page.
#0 0x55faed39dd7e in jsP_dumpsyntax /benchmark/mujs/jsdump.c:685
#1 0x55faed3ea327 in js_ppstring /benchmark/mujs/pp.c:24
#2 0x55faed3ea704 in js_ppfile /benchmark/mujs/pp.c:77
#3 0x55faed3ea985 in main /benchmark/mujs/pp.c:106
#4 0x7f5c97280d8f (/lib/x86_64-linux-gnu/libc.so.6+0x2dd8f)
#5 0x7f5c97280e3f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2de3f)
#6 0x55faed3849c4 in _start (/benchmark/mujs/build/sanitize/mujs-pp+0x169c4)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /benchmark/mujs/jsdump.c:685 in jsP_dumpsyntax
==1412001==ABORTING
```

POC for bug 2

[crash.zip](#)

Credit


Han Zheng ([NCNIPC of China](#), [Hexhive](#))
Yin Li, Xiaotong Jiao (NCNIPC of China)

 **ccxvii** added a commit that referenced this issue on May 17



Issue [#161](#): Don't fclose a FILE that is NULL.

910acc8

 **ccxvii** added a commit that referenced this issue on May 17



Issue [#161](#): Cope with empty programs in mujs-pp.

f5b3c70



ccxvii closed this as completed on May 17

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

