New issue

Jump to bottom

A NULL pointer dereference in the function json_printf() mjs.c:6396 #161

⊙ Open **Clingto** opened this issue on May 19, 2021 · 0 comments

Clingto commented on May 19, 2021

System info:
Ubuntu 16.04.6 LTS, X64, gcc 5.4.0, mjs (latest master `4c870e5`)
Compile Command:

```
$ gcc -fsanitize=address -fno-omit-frame-pointer -DMJS_MAIN mjs.c -ldl -g -o mjs
```

Run Command:

```
$ mjs -f $POC
```

POC file:
https://github.com/Clingto/POC/blob/master/MSA/mjs/mjs-6368-json_printf-null-pointer-deref

ASAN info:

```
ASAN:SIGSEGV
=================================================================
==31649==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x00000040e9b8 bp 0x7fff1c80ad38 sp 0x7fff1c80abe8 T0)
    #0 0x40e9b7 in json_printf  test/mjs-uaf/build_asan/mjs.c:6396
    #1 0x444aee in mjs_jprintf  test/mjs-uaf/build_asan/mjs.c:14741
    #2 0x44511a in mjs_fprintf  test/mjs-uaf/build_asan/mjs.c:14781
    #3 0x41dd43 in mjs_print  test/mjs-uaf/build_asan/mjs.c:8088
    #4 0x7fff1c80af6f  (<unknown module>)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV  test/mjs-uaf/build_asan/mjs.c:6396 json_printf
==31649==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant