A NULL pointer dereference in the function mjs_string_char_code_at() mjs.c:14234 #169

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-13891-mjs_string_char_code_at-null-pointer-deref

ASAN info:

```
ASAN:SIGSEGV
=================================================================
==28983==ERROR: AddressSanitizer: SEGV on unknown address 0x618008111179 (pc 0x000000440f53 bp 0x7ffe126104c0 sp 0x7ffe126103c0 T0)
    #0 0x440f52 in mjs_string_char_code_at  test/mjs-uaf/build_asan/mjs.c:14234
    #1 0x42572a in mjs_execute  test/mjs-uaf/build_asan/mjs.c:9648
    #2 0x4265f1 in mjs_exec_internal  test/mjs-uaf/build_asan/mjs.c:9866
    #3 0x426873 in mjs_exec_file  test/mjs-uaf/build_asan/mjs.c:9889
    #4 0x431348 in main  test/mjs-uaf/build_asan/mjs.c:12228
    #5 0x7fbb2940582f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #6 0x401af8 in _start ( test/mjs-uaf/bin_asan/bin/mjs_bin+0x401af8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV  test/mjs-uaf/build_asan/mjs.c:14234 mjs_string_char_code_at
==28983==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant