New issue

Jump to bottom

AddressSanitizer: 1 memory leaks of frozen_cb() #160

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-5794-frozen_cb-memory-leak

ASAN info:

```
==29407==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 37331 byte(s) in 1 object(s) allocated from:
    #0 0x7f151fe52602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
    #1 0x42ffcd in frozen_cb  test/mjs-uaf/build_asan/mjs.c:12025
    #2 0x4092c4 in json_parse_string  test/mjs-uaf/build_asan/mjs.c:5898
    #3 0x40b482 in json_parse_value  test/mjs-uaf/build_asan/mjs.c:5993
    #4 0x40aa25 in json_parse_array  test/mjs-uaf/build_asan/mjs.c:5958
    #5 0x40b4c4 in json_parse_value  test/mjs-uaf/build_asan/mjs.c:6000
    #6 0x40b863 in json_parse_pair  test/mjs-uaf/build_asan/mjs.c:6058
    #7 0x40bc63 in json_parse_object  test/mjs-uaf/build_asan/mjs.c:6070
    #8 0x40b4a3 in json_parse_value  test/mjs-uaf/build_asan/mjs.c:5996
    #9 0x40c135 in json_doit  test/mjs-uaf/build_asan/mjs.c:6083
    #10 0x40f2aa in json_walk  test/mjs-uaf/build_asan/mjs.c:6466
    #11 0x4309d9 in mjs_json_parse  test/mjs-uaf/build_asan/mjs.c:12133
    #12 0x430f11 in mjs_op_json_parse  test/mjs-uaf/build_asan/mjs.c:12193
    #13 0x42572a in mjs_execute  test/mjs-uaf/build_asan/mjs.c:9648
    #14 0x4265f1 in mjs_exec_internal  test/mjs-uaf/build_asan/mjs.c:9866
    #15 0x426873 in mjs_exec_file  test/mjs-uaf/build_asan/mjs.c:9889
    #16 0x431348 in main  test/mjs-uaf/build_asan/mjs.c:12228
    #17 0x7f151f80c82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)

SUMMARY: AddressSanitizer: 37331 byte(s) leaked in 1 allocation(s).
```

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant