


New issue

[Jump to bottom](#)

AddressSanitizer: stack-buffer-overflow in mjs_execute mjs.c:9650 #167

 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-9522-mjs_execute-stack-overflow

ASAN info:

```
ASAN:SIGSEGV
=====
==9792==ERROR: AddressSanitizer: stack-overflow on address 0x7ffc50dbbc70 (pc 0x000000425735 bp 0x7ffc50dafdf0 sp 0x7ffc50dbbc78 T0)
#0 0x425734 in mjs_execute test/mjs-uaf/build_asan/mjs.c:9650
#1 0x4265f1 in mjs_exec_internal test/mjs-uaf/build_asan/mjs.c:9866
#2 0x426873 in mjs_exec_file test/mjs-uaf/build_asan/mjs.c:9889
#3 0x431348 in main test/mjs-uaf/build_asan/mjs.c:12228
#4 0x7fa093d7e82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#5 0x401af8 in _start (test/mjs-uaf/bin_asan/bin/mjs_bin+0x401af8)

SUMMARY: AddressSanitizer: stack-overflow test/mjs-uaf/build_asan/mjs.c:9650 mjs_execute
==9792==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

