New issue

Jump to bottom

A NULL pointer dereference in the function mjs_bcode_part_get_by_offset() mjs.c:8042 #162

⊙ 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-7945-mjs_bcode_part_get_by_offset-null-pointer-deref

ASAN info:

```
ASAN:SIGSEGV
=================================================================
==7862==ERROR: AddressSanitizer: SEGV on unknown address 0x00000041bd8c (pc 0x00000041da25 bp 0x7ffcdf11d400 sp 0x7ffcdf11d138 T0)
    #0 0x41da24 in mjs_bcode_part_get_by_offset  test/mjs-uaf/build_asan/mjs.c:8042
    #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 0x7f524fe1682f 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)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV  test/mjs-uaf/build_asan/mjs.c:8042 mjs_bcode_part_get_by_offset
==7862==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant