New issue

Jump to bottom

AddressSanitizer: stack-buffer-overflow in <unknown module> #170

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-module-stack-overflow

ASAN info:

```
ASAN:SIGSEGV
=================================================================
==10560==ERROR: AddressSanitizer: stack-overflow on address 0x7fffe9049390 (pc 0x7fffe9049390 bp 0x00000042572b sp 0x7fffe9049348 T0)
    #0 0x7fffe904938f  (<unknown module>)

SUMMARY: AddressSanitizer: stack-overflow ??:0 ??
==10560==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant