AddressSanitizer: negative-size-param in gc_compact_strings() mjs.c:11575 #159

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-8d05d-gc_compact_strings-negative-size-param

ASAN info:

```
==10043==ERROR: AddressSanitizer: negative-size-param: (size=-2133205735)
    #0 0x7f03ca4b105d in __asan_memmove (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x8d05d)
    #1 0x42dd05 in gc_compact_strings  test/mjs-uaf/build_asan/mjs.c:11575
    #2 0x42e26a in mjs_gc  test/mjs-uaf/build_asan/mjs.c:11646
    #3 0x42df57 in maybe_gc  test/mjs-uaf/build_asan/mjs.c:11592
    #4 0x424572 in mjs_execute  test/mjs-uaf/build_asan/mjs.c:9375
    #5 0x4265f1 in mjs_exec_internal  test/mjs-uaf/build_asan/mjs.c:9866
    #6 0x426873 in mjs_exec_file  test/mjs-uaf/build_asan/mjs.c:9889
    #7 0x431348 in main  test/mjs-uaf/build_asan/mjs.c:12228
    #8 0x7f03c9e7682f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #9 0x401af8 in _start ( test/mjs-uaf/bin_asan/bin/mjs_bin+0x401af8)

0x7f01c397fe41 is located 2702202433 bytes inside of 4863964088-byte region [0x7f012287a800,0x7f024471dbb8)
allocated by thread T0 here:
    #0 0x7f03ca4bc961 in realloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98961)
    #1 0x402baa in mbuf_resize  test/mjs-uaf/build_asan/mjs.c:4878
    #2 0x43f0fb in mjs_mk_string  test/mjs-uaf/build_asan/mjs.c:13934
    #3 0x4403f9 in s_concat  test/mjs-uaf/build_asan/mjs.c:14115
    #4 0x422362 in do_op  test/mjs-uaf/build_asan/mjs.c:8996
    #5 0x42247a in op_assign  test/mjs-uaf/build_asan/mjs.c:9009
    #6 0x4231f9 in exec_expr  test/mjs-uaf/build_asan/mjs.c:9212
    #7 0x4259f6 in mjs_execute  test/mjs-uaf/build_asan/mjs.c:9683
    #8 0x4265f1 in mjs_exec_internal  test/mjs-uaf/build_asan/mjs.c:9866
    #9 0x426873 in mjs_exec_file  test/mjs-uaf/build_asan/mjs.c:9889
    #10 0x431348 in main  test/mjs-uaf/build_asan/mjs.c:12228
    #11 0x7f03c9e7682f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)

SUMMARY: AddressSanitizer: negative-size-param ??:0 __asan_memmove
==10043==ABORTING
```

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant