

[New issue](#)[Jump to bottom](#)

AddressSanitizer: stack-overflow on recursive stack frames: parse_block, parse_statement, parse_statement_list #135

🔒 Closed wcvventure opened this issue on May 28, 2019 · 1 comment

wcvventure commented on May 28, 2019

An issue was discovered in mjs.c 1.20.1. Stack Exhaustion occurs in mjs_mk_string function, and there is a stack consumption problem caused by recursive stack frames

POC:

[POC.zip](#)

ASAN output:

```
AddressSanitizer:DEADLYSIGNAL
=====
==22443==ERROR: AddressSanitizer: stack-overflow on address 0x7ffc66adaa38 (pc 0x0000004dd9cf bp 0x7ffc66adb2b0 sp 0x7ffc66adaa40 T0)
#0 0x4dd9ce in __asan_memmove /home/hjwang/Tools/llvm-6.0.1/projects/compiler-rt/lib/asan/asan_interceptors_memintrinsics.cc:31
#1 0x517ab8 in mbuf_insert /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:4790:5
#2 0x5945c2 in emit_byte /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:7672:3
#3 0x5945c2 in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12203
#4 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#5 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#6 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#7 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#8 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#9 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#10 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#11 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#12 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#13 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#14 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#15 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#16 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#17 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#18 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#19 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#20 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#21 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#22 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#23 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#24 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#25 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#26 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#27 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#28 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#29 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#30 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#31 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#32 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#33 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#34 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#35 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#36 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#37 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#38 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#39 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#40 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#41 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#42 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#43 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#44 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#45 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#46 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#47 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#48 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#49 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#50 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#51 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#52 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#53 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#54 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#55 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#56 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#57 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#58 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#59 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#60 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#61 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#62 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#63 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#64 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#65 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#66 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#67 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#68 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#69 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#70 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#71 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#72 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#73 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#74 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#75 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#76 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#77 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#78 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#79 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#80 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
```

[illegible]

```
#194 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#195 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#196 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#197 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#198 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#199 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#200 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#201 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#202 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#203 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#204 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#205 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#206 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#207 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#208 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#209 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#210 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#211 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#212 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#213 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#214 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#215 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#216 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#217 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#218 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#219 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#220 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#221 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#222 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#223 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#224 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#225 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#226 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#227 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#228 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#229 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#230 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#231 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#232 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#233 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#234 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#235 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#236 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#237 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#238 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#239 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#240 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#241 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#242 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#243 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#244 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#245 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#246 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#247 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
#248 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#249 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12204:9
#250 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14
```

SUMMARY: AddressSanitizer: stack-overflow /home/hjwang/Tools/llvm-6.0.1/projects/compiler-rt/lib/asan/asan_interceptors_memintrinsics.cc:31 in __asan_memmove
==22443==ABORTING

wcventure commented on May 31, 2019

Author

Fixed In latest version.



wcventure closed this as completed on May 31, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

