Jump to bottom New issue

## AddressSanitizer: stack-overflow on recursive stack frames: parse\_block, parse\_statement, parse\_statement\_list #135

⊙ Closed ) wcventure opened this issue on May 28, 2019 · 1 comment

wcventure commented on May 28, 2019 An issue was discovered in mis.c 1.20.1. Stack Exhaustion occurs in mis mk string function, and there is a stack consumption problem caused by recursive stack frames POC.zin ASAN output: AddressSanitizer: DEADLYSIGNA ==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\_afl\_asan/mjs.c:4790:5
#2 0x5945c2 in emit\_byte /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:7672:3 #3 0x5945c2 in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12203 #4 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 ## 5 %x57941 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11
#6 %x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9
#7 %x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12214:14
#8 %x57941 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11
#9 %x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #10 0x588dda in parse\_statement /home/hjwang/UAF\_objects/mjs\_afl\_asan/mjs.c:12914:14
#11 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #11 0x576914 in parse\_Statement\_list /nome/njwang/UAF\_Dujects/mjs\_afl\_asan/mjs.c:12294:9
#13 0x588dda in parse\_statement /home/hjwang/UAF\_Dujects/mjs\_afl\_asan/mjs.c:12294:14
#14 0x576914 in parse\_statement\_list /home/hjwang/UAF\_Dujects/mjs\_afl\_asan/mjs.c:122914:14
#14 0x576916 in parse\_statement\_list /home/hjwang/UAF\_Dujects/mjs\_afl\_asan/mjs.c:12294:19
#16 0x588dda in parse\_statement /home/hjwang/UAF\_Dujects/mjs\_afl\_asan/mjs.c:12294:14 #17 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #18 0x59462f in parse block /home/hjwang/UAF Objects/mjs afl asan/mjs.c:12204:9 #19 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14
#20 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #21 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9
#22 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #23 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #24 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #25 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14
#26 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #27 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #28 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #29 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #30 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #31 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14
#32 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11
#33 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #34 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #35 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #36 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #37 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #38 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #39 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #40 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #41 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #42 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #43 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #44 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #45 0x59462f in parse\_block /home/hjwang/UAF\_0bjects/mjs\_afl\_asan/mjs.c:12204:9 #46 0x588dda in parse\_statement /home/hjwang/UAF\_0bjects/mjs\_afl\_asan/mjs.c:12914:14 #47 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #48 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #49 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #50 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #51 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #52 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #53 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #54 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #55 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #56 0x57f914 in parse statement list /home/hiwang/UAF Objects/mis afl asan/mis.c:12193:11 #57 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #58 0x588dda in parse\_statement /home/hjwang/UAF\_0bjects/mjs\_afl\_asan/mjs.c:12914:14 #59 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_0bjects/mjs\_afl\_asan/mjs.c:12193:11 #60 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #61 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #62 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #63 0x59462f in parse\_block /home/hjwang/UAF\_0bjects/mjs\_afl\_asan/mjs.c:12204:9 #64 0x588dda in parse\_statement /home/hjwang/UAF\_0bjects/mjs\_afl\_asan/mjs.c:12914:14 #65 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_0bjects/mjs\_afl\_asan/mjs.c:12193:11 #66 0x59462f in parse\_block /home/hjwang/UAF\_0bjects/mjs\_afl\_asan/mjs.c:12204:9 #67 0x588dda in parse\_statement /home/hjwang/UAF\_0bjects/mjs\_afl\_asan/mjs.c:12914:14 #68 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #69 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #70 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #71 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #72 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9
#73 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #74 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #75 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #76 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14
#77 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #78 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #79 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14
#80 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11

```
#81 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#82 0x588dda in parse statement /home/hjwang/UAF Objects/mjs afl asan/mjs.c:12914:14
#83 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11 #84 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#85 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14 #86 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#87 0x59462f in parse_block /home/hjwang/UAF_0bjects/mjs_afl_asan/mjs.c:12204:9 #88 0x588dda in parse_statement /home/hjwang/UAF_0bjects/mjs_afl_asan/mjs.c:12914:14
#89 0x57f914 in parse statement list /home/hjwang/UAF Objects/mjs afl asan/mjs.c:12193:11
#90 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#91 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#92 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#93 0x59462f in parse block /home/hjwang/UAF Objects/mjs afl asan/mjs.c:12204:9
#94 0x588dda in parse_statement_/home/hjwang/UAF_0bjects/mjs_afl_asan/mjs.c:12914:14 #95 0x57f914 in parse_statement_list /home/hjwang/UAF_0bjects/mjs_afl_asan/mjs.c:12193:11
#96 0x59462f in parse block /home/hjwang/UAF Objects/mjs afl asan/mjs.c:12204:9
#97 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#98 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#99 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#100 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#101 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11 #102 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#103 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#104 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#105 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#106 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#107 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#108 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#109 0x588dda in parse_statement /home/hjwang/UAF_0bjects/mjs_afl_asan/mjs.c:12914:14
#110 0x57f914 in parse_statement_list /home/hjwang/UAF_0bjects/mjs_afl_asan/mjs.c:12193:11
#111 0x59462f in parse block /home/hjwang/UAF Objects/mjs afl asan/mjs.c:12204:9
#112 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#113 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#114 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#115 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#116 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#117 0x59462f in parse_block /home/hjwang/UAF_objects/mjs_afl_asan/mjs.c:12204:9
#118 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#119 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11 #120 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#121 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#122 0x57f914 in parse statement list /home/hjwang/UAF Objects/mjs afl asan/mjs.c:12193:11
#123 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#124 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#125 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#126 0x59462f in parse_block /home/hjwang/UAF_objects/mjs_afl_asan/mjs.c:12204:9
#127 0x588dda in parse_statement /home/hjwang/UAF_0bjects/mjs_afl_asan/mjs.c:12914:14
#128 0x57f914 in parse_statement_list /home/hjwang/UAF_0bjects/mjs_afl_asan/mjs.c:12193:11
#129 0x59462f in parse block /home/hjwang/UAF Objects/mjs afl asan/mjs.c:12204:9
#130 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12914:14 #131 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#132 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#133 0x588dda in parse statement /home/hjwang/UAF Objects/mjs afl asan/mjs.c:12914:14
#134 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11 #135 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#136 0x588dda in parse_statement /home/hjwang/UAF_0bjects/mjs_afl_asan/mjs.c:12914:14
#137 0x57f914 in parse_statement_list /home/hjwang/UAF_0bjects/mjs_afl_asan/mjs.c:12193:11
#138 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#139 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#140 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#141 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:5
#142 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#143 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11 #144 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#145 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#146 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#147 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#148 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#149 @x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11 #150 @x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#151 0x588dda in parse_statement /home/hjwang/UAF_0bjects/mjs_afl_asan/mjs.c:12914:14
#152 0x57f914 in parse_statement_list /home/hjwang/UAF_0bjects/mjs_afl_asan/mjs.c:12193:11
#153 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#154 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14 #155 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#156 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#157 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#158 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11 #159 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#160 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#161 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#162 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#163 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#164 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#165 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#166 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#167 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11 #168 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#169 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#170 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#171 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#172 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#173 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#174 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#175 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#176 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#177 0x59462f in parse_block /home/hjwang/UAF_objects/mjs_afl_asan/mjs.c:12204:9
#178 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#179 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#180 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#181 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#182 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#183 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#184 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#185 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12193:11
#186 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#187 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#188 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#189 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#190 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
#191 0x57f914 in parse_statement_list /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12193:11
#192 0x59462f in parse_block /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12204:9
#193 0x588dda in parse_statement /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12914:14
```

#194 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #195 0x59462f in parse block /home/hjwang/UAF Objects/mjs afl asan/mjs.c:12204:9 #196 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #197 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #198 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9
#199 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #200 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #201 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #202 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #203 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #204 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #205 0x588dda in parse\_statement /home/hjwang/UAF\_0bjects/mjs\_afl\_asan/mjs.c:12914:14
#206 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_0bjects/mjs\_afl\_asan/mjs.c:12193:11 #207 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9
#208 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #209 0x57f914 in parse statement list /home/hjwang/UAF Objects/mjs afl asan/mjs.c:12193:11 #210 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #211 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14
#212 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #213 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #214 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #215 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #216 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9
#217 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #218 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11
#219 0x59462f in parse\_block /home/hjwang/UAF\_objects/mjs\_afl\_asan/mjs.c:12204:9 #220 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #221 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #222 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9
#223 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #224 0x57f914 in parse statement list /home/hjwang/UAF Objects/mjs afl asan/mjs.c:12193:11 #225 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9
#226 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #227 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11
#228 0x59462f in parse\_block /home/hjwang/UAF\_objects/mjs\_afl\_asan/mjs.c:12204:9 #229 0x588dda in parse\_statement /home/hjwang/UAF\_0bjects/mjs\_afl\_asan/mjs.c:12914:14
#230 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_0bjects/mjs\_afl\_asan/mjs.c:12193:11 #231 %59462f in parse\_block /home/hjwang/UAF\_objects/mjs\_afl\_asan/mjs.c:12914:14
#232 %588dda in parse\_statement /home/hjwang/UAF\_objects/mjs\_afl\_asan/mjs.c:12914:14
#233 %57f914 in parse\_statement\_list /home/hjwang/UAF\_objects/mjs\_afl\_asan/mjs.c:12193:11 #234 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #235 0x588dda in parse statement /home/hjwang/UAF Objects/mjs afl asan/mjs.c:12914:14 #236 0x574914 in parse\_statement\_list\_/home/hjwang/UAF\_objects/mjs\_efl\_asan/mjs.c:12193:11 #237 0x59462f in parse\_block /home/hjwang/UAF\_objects/mjs\_afl\_asan/mjs.c:12204:9 #238 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14
#239 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #240 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #241 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #242 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #243 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #244 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #245 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #246 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9 #247 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12914:14 #248 0x57f914 in parse\_statement\_list /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12193:11 #249 0x59462f in parse\_block /home/hjwang/UAF\_Objects/mjs\_afl\_asan/mjs.c:12204:9
#250 0x588dda in parse\_statement /home/hjwang/UAF\_Objects/mjs\_afl\_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

Projects None yet

Milestone

No milestone

Development

No branches or pull requests

l participant

