AddressSanitizer: stack-overflow on recursive stack frames: parse_unary, parse_mul_div_rem, parse_plus_minus... #136

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

wcventure commented on May 28, 2019

POC:
POC.zip

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==23779==ERROR: AddressSanitizer: stack-overflow on address 0x7ffcd8b22f68 (pc 0x0000005a63b8 bp 0x7ffcd8b23110 sp 0x7ffcd8b22f68 T0)
    #0 0x5a63b7 in findtok /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12117:25
    #1 0x5a63b7 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12426
    #2 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
    #3 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
    #4 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
    #5 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
    #6 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
    #7 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
    #8 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
    #9 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
    #10 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3
    #11 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12489:3
    #12 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12494:14
    #13 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12532:3
    #14 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12536:10
    #15 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12294
    #16 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12354:13
    #17 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12380
    #18 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12414:14
    #19 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12433
    #20 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
    #21 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
    #22 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
    #23 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
    #24 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
    #25 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
    #26 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
    #27 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
    #28 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3
    #29 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12489:3
    #30 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12494:14
    #31 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12532:3
    #32 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12536:10
    #33 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12294
    #34 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12354:13
    #35 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12380
    #36 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12414:14
    #37 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12433
    #38 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
    #39 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
    #40 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
    #41 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
    #42 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
    #43 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
    #44 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
    #45 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
    #46 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3
    #47 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12489:3
    #48 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12494:14
    #49 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12532:3
    #50 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12536:10
    #51 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12294
    #52 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12354:13
    #53 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12380
    #54 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12414:14
    #55 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12433
    #56 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
    #57 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
    #58 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
    #59 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
    #60 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
    #61 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
    #62 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
    #63 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
    #64 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3
    #65 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12489:3
    #66 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12494:14
    #67 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12532:3
    #68 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12536:10
    #69 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12294
    #70 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12354:13
    #71 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12380
    #72 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12414:14
    #73 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12433
    #74 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
    #75 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
    #76 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
    #77 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
    #78 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
    #79 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
    #80 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
    #81 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
    #82 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3
    #83 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12489:3
    #84 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12494:14
```

```
#85 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12532:3
#86 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12536:10
#87 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12294
#88 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12354:13
#89 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12380
#90 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12414:14
#91 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12433
#92 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
#93 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
#94 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
#95 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
#96 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
#97 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
#98 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
#99 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
#100 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3
#101 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12489:3
#102 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12494:14
#103 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12532:3
#104 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12536:10
#105 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12294
#106 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12354:13
#107 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12380
#108 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12414:14
#109 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12433
#110 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
#111 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
#112 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
#113 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
#114 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
#115 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
#116 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
#117 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
#118 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3
#119 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12489:3
#120 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12494:14
#121 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12532:3
#122 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12536:10
#123 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12294
#124 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12354:13
#125 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12380
#126 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12414:14
#127 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12433
#128 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
#129 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
#130 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
#131 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
#132 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
#133 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
#134 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
#135 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
#136 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3
#137 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12489:3
#138 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12494:14
#139 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12532:3
#140 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12536:10
#141 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12294
#142 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12354:13
#143 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12380
#144 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12414:14
#145 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12433
#146 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
#147 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
#148 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
#149 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
#150 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
#151 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
#152 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
#153 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
#154 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3
#155 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12489:3
#156 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12494:14
#157 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12532:3
#158 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12536:10
#159 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12294
#160 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12354:13
#161 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12380
#162 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12414:14
#163 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12433
#164 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
#165 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
#166 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
#167 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
#168 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
#169 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
#170 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
#171 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
#172 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3
#173 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12489:3
#174 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12494:14
#175 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12532:3
#176 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12536:10
#177 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12294
#178 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12354:13
#179 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12380
#180 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12414:14
#181 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12433
#182 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
#183 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
#184 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
#185 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
#186 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
#187 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
#188 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
#189 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
#190 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3
#191 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12489:3
#192 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12494:14
#193 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12532:3
#194 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12536:10
#195 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12294
#196 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12354:13
#197 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12380
```

```
    #198 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12414:14
    #199 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12433
    #200 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
    #201 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
    #202 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
    #203 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
    #204 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
    #205 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
    #206 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
    #207 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
    #208 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3
    #209 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12489:3
    #210 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12494:14
    #211 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12532:3
    #212 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12536:10
    #213 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12294
    #214 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12354:13
    #215 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12380
    #216 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12414:14
    #217 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12433
    #218 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
    #219 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
    #220 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
    #221 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
    #222 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
    #223 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
    #224 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
    #225 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
    #226 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3
    #227 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12489:3
    #228 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12494:14
    #229 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12532:3
    #230 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12536:10
    #231 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12294
    #232 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12354:13
    #233 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12380
    #234 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12414:14
    #235 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12433
    #236 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
    #237 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
    #238 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
    #239 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
    #240 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
    #241 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
    #242 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
    #243 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
    #244 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3
    #245 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12489:3
    #246 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12494:14
    #247 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12532:3
    #248 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12536:10
    #249 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12294
    #250 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12354:13
    #251 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12380
    #252 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12414:14
    #253 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12433
    #254 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
    #255 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
    #256 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
    #257 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
    #258 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
    #259 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
    #260 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
    #261 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
    #262 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3
    #263 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12489:3
    #264 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12494:14
    #265 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12532:3
    #266 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12536:10
    #267 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12294
    #268 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12354:13
    #269 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12380
    #270 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12414:14
    #271 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12433
    #272 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
    #273 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
    #274 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
    #275 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
    #276 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
    #277 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
    #278 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
    #279 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
    #280 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3
    #281 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12489:3
    #282 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12494:14
    #283 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12532:3
    #284 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12536:10
    #285 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12294
    #286 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12354:13
    #287 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12380
    #288 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12414:14
    #289 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12433
    #290 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12446:3
    #291 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12451:3
    #292 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12456:3
    #293 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12460:3
    #294 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12464:3
    #295 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12469:3
    #296 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12474:3
    #297 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12479:3
    #298 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12484:3

SUMMARY: AddressSanitizer: stack-overflow /home/hjwang/UAF_Objects/mjs_afl_asan/mjs.c:12117:25 in findtok
==23779==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