

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

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

🔒 Closed

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

wcvventure 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_af1_asan/mjs.c:12117:25
#1 0x5a63b7 in parse_unary /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12426
#2 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12446:3
#3 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12451:3
#4 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12456:3
#5 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12460:3
#6 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12464:3
#7 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12469:3
#8 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12474:3
#9 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12479:3
#10 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12484:3
#11 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12489:3
#12 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12494:14
#13 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12532:3
#14 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12536:10
#15 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12294
#16 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12354:13
#17 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12380
#18 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12414:14
#19 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12433
#20 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12446:3
#21 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12451:3
#22 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12456:3
#23 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12460:3
#24 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12464:3
#25 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12469:3
#26 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12474:3
#27 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12479:3
#28 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12484:3
#29 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12489:3
#30 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12494:14
#31 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12532:3
#32 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12536:10
#33 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12294
#34 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12354:13
#35 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12380
#36 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12414:14
#37 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12433
#38 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12446:3
#39 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12451:3
#40 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12456:3
#41 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12460:3
#42 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12464:3
#43 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12469:3
#44 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12474:3
#45 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12479:3
#46 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12484:3
#47 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12489:3
#48 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12494:14
#49 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12532:3
#50 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12536:10
#51 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12294
#52 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12354:13
#53 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12380
#54 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12414:14
#55 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12433
#56 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12446:3
#57 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12451:3
#58 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12456:3
#59 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12460:3
#60 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12464:3
#61 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12469:3
#62 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12474:3
#63 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12479:3
#64 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12484:3
#65 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12489:3
#66 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12494:14
#67 0x599c92 in parse_assignment /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12532:3
#68 0x5acfb4 in parse_expr /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12536:10
#69 0x5acfb4 in parse_array_literal /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12294
#70 0x5a7a58 in parse_literal /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12354:13
#71 0x5a7a58 in parse_call_dot_mem /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12380
#72 0x5a6400 in parse_postfix /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12414:14
#73 0x5a6400 in parse_unary /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12433
#74 0x5a5a6e in parse_mul_div_rem /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12446:3
#75 0x5a5236 in parse_plus_minus /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12451:3
#76 0x5a4b00 in parse_shifts /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12456:3
#77 0x5a441e in parse_comparison /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12460:3
#78 0x5a3c4f in parse_equality /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12464:3
#79 0x5a24ab in parse_bitwise_and /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12469:3
#80 0x5a0bec in parse_bitwise_xor /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12474:3
#81 0x59f1ab in parse_bitwise_or /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12479:3
#82 0x59d944 in parse_logical_and /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12484:3
#83 0x59c593 in parse_logical_or /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12489:3
#84 0x59a5f1 in parse_ternary /home/hjwang/UAF_Objects/mjs_af1_asan/mjs.c:12494:14
```

[illegible]

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

==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

