


New issue

[Jump to bottom](#)

## AddressSanitizer: heap-use-after-free in expr\_traverse\_nodes\_post() libyasm/expr.c:1112 #165

 Open Clingo 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, yasm (latest master [009450c](#) )I think it is probably a similar issue as [#126](#)

Compile Command:

```
$ ./autogen.sh
make distclean

CC=gcc CXX=g++ CFLAGS="-fsanitize=address -fno-omit-frame-pointer -g" CXXFLAGS="-fsanitize=address -fno-omit-frame-pointer -g" ./configure --prefix=$PWD/build --disable-shared
make -j
make install
```

Run Command:

```
$ yasm $POC
```

POC file:

[https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-1226-expr\\_traverse\\_nodes\\_post-UAF](https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-1226-expr_traverse_nodes_post-UAF)

ASAN info:

```
yasm: file name already has no extension: output will be in `yasm.out'
=====
==11980==ERROR: AddressSanitizer: heap-use-after-free on address 0x6060000e5b0 at pc 0x7f418ef4a94b bp 0x7ffedeadea70 sp 0x7ffedeadea60
READ of size 4 at 0x6060000e5b0 thread T0
#0 0x7f418ef4a94a in expr_traverse_nodes_post test/yasm-uaf/SRC_asan/libyasm/expr.c:1112
#1 0x7f418ef4a94a in yasm_expr_destroy test/yasm-uaf/SRC_asan/libyasm/expr.c:1045
#2 0x7f418ef7ebd1 in bin_section_data_destroy test/yasm-uaf/SRC_asan/modules/objfmts/bin/bin-objfmt.c:1684
#3 0x7f418ef2e548 in yasm__assoc_data_destroy test/yasm-uaf/SRC_asan/libyasm/assocdat.c:128
#4 0x7f418ef6dd24 in yasm_section_destroy test/yasm-uaf/SRC_asan/libyasm/section.c:676
#5 0x7f418ef6dd24 in yasm_object_destroy test/yasm-uaf/SRC_asan/libyasm/section.c:470
#6 0x404ad4 in cleanup test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:799
#7 0x4053e3 in check_errors test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:778
#8 0x402c9a in do_assemble test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:524
#9 0x402c9a in main test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:753
#10 0x7f418e96f82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#11 0x403ee8 in _start ( test/yasm-uaf/bin_asan/bin/yasm+0x403ee8)

0x6060000e5b0 is located 16 bytes inside of 56-byte region [0x6060000e5a0,0x6060000e5d8)
freed by thread T0 here:
#0 0x7f418f2292ca in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x982ca)
#1 0x7f418ef76caa in yasm_dir_helper_expr test/yasm-uaf/SRC_asan/libyasm/valparam.c:312
#2 0x7f418ef769ff in yasm_dir_helper test/yasm-uaf/SRC_asan/libyasm/valparam.c:241
#3 0x7f418b7eb34b in bin_objfmt_section_switch test/yasm-uaf/SRC_asan/modules/objfmts/bin/bin-objfmt.c:1521
#4 0x7f418ef6cd75 in dir_section test/yasm-uaf/SRC_asan/libyasm/section.c:154
#5 0x7f418ef6d838 in yasm_object_directive test/yasm-uaf/SRC_asan/libyasm/section.c:377
#6 0x7f418b78f804 in nasm_parser_directive test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:1569
#7 0x7f418b79bd3c in parse_line test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:377
#8 0x7f418b79bd3c in nasm_parser_parse test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:231
#9 0x7f418b78f36b in nasm_do_parse test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:66
#10 0x7f418b78f36b in nasm_parser_do_parse test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:83
#11 0x402c84 in do_assemble test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:521
#12 0x402c84 in main test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:753
#13 0x7f418e96f82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)

previously allocated by thread T0 here:
#0 0x7f418f229602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
#1 0x7f418ef7a769 in def_xmalloc test/yasm-uaf/SRC_asan/libyasm/xmalloc.c:69
#2 0x7f418ef46fd2 in yasm_expr__copy_except test/yasm-uaf/SRC_asan/libyasm/expr.c:998
#3 0x7f418ef76cd0 in yasm_dir_helper_expr test/yasm-uaf/SRC_asan/libyasm/valparam.c:313
#4 0x7f418ef769ff in yasm_dir_helper test/yasm-uaf/SRC_asan/libyasm/valparam.c:241
#5 0x7f418b7eb34b in bin_objfmt_section_switch test/yasm-uaf/SRC_asan/modules/objfmts/bin/bin-objfmt.c:1521
#6 0x7f418ef6cd75 in dir_section test/yasm-uaf/SRC_asan/libyasm/section.c:154
#7 0x7f418ef6d838 in yasm_object_directive test/yasm-uaf/SRC_asan/libyasm/section.c:377
#8 0x7f418b78f804 in nasm_parser_directive test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:1569
#9 0x7f418b79bd3c in parse_line test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:377
#10 0x7f418b79bd3c in nasm_parser_parse test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:231
#11 0x7f418b78f36b in nasm_do_parse test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:66
#12 0x7f418b78f36b in nasm_parser_do_parse test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:83
#13 0x402c84 in do_assemble test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:521
#14 0x402c84 in main test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:753
#15 0x7f418e96f82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)

SUMMARY: AddressSanitizer: heap-use-after-free test/yasm-uaf/SRC_asan/libyasm/expr.c:1112 expr_traverse_nodes_post
Shadow bytes around the buggy address:
 0x0c0c7fff9c60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c0c7fff9c70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c0c7fff9c80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c0c7fff9c90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c0c7fff9ca0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
=>0x0c0c7fff9cb0: fa fa fa fa fd fd[fd]fd fd fd fd fa fa fa fa fa
 0x0c0c7fff9cc0: fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd fd
 0x0c0c7fff9cd0: fd fd fd fa fa fa fa fa fd fd fd fd fd fd fd fa
 0x0c0c7fff9ce0: fa fa fa fa fd fd fd fd fd fd fa fa fa fa fa fa
 0x0c0c7fff9cf0: fd fd fd fd fd fd fa fa fa fa fa fd fd fd fd fd
 0x0c0c7fff9d00: fd fd fd fa fa fa fa fa fd fd fd fd fd fd fd fd
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable: 00
```

```
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:    fa
Heap right redzone:   fb
Freed heap region:    fd
Stack left redzone:   f1
Stack mid redzone:    f2
Stack right redzone:  f3
Stack partial redzone: f4
Stack after return:   f5
Stack use after scope: f8
Global redzone:       f9
Global init order:    f6
Poisoned by user:     f7
Container overflow:   fc
Array cookie:         ac
Intra object redzone: bb
ASan internal:         fe
==11980==ABORTING
```



  natalie13m mentioned this issue on Nov 1, 2021

Stack overflow in parse\_expr6(5,4,3,2,1) modules/parsers/nasm/nasm-parse.c #152

 Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

