

New issue

[Jump to bottom](#)

## A NULL pointer dereference in the function nasm\_parser\_directive() modules/parsers/nasm/nasm-parse.c:1596 #167

Open Clingto 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](#) )

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-1595-nasm\\_parser\\_directive-null-pointer-deref](https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-1595-nasm_parser_directive-null-pointer-deref)

ASAN info:

```
yasm: file name already has no extension: output will be in `yasm.out`
ASAN:SIGSEGV
=====
==13148==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f3a60e8fbb7 bp 0x7fff5f933810 sp 0x7fff5f933720 T0)
#0 0x7f3a60e8fbb6 in nasm_parser_directive test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:1596
#1 0x7f3a60e9bd3c in parse_line test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:377
#2 0x7f3a60e9bd3c in nasm_parser_parse test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:231
#3 0x7f3a60e8f36b in nasm_do_parse test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:66
#4 0x7f3a60e8f36b in nasm_parser_do_parse test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:83
#5 0x402c84 in do_assemble test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:521
#6 0x402c84 in main test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:753
#7 0x7f3a6405182f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#8 0x403ee8 in _start (test/yasm-uaf/bin_asan/bin/yasm+0x403ee8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:1596 nasm_parser_directive
==13148==ABORTING
```

1

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

