A NULL pointer dereference in the function expand_mmacro() modules/preprocs/nasm/nasm-pp.c:4764 #173

⊙ 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-4760-expand_mmacro-null-pointer-deref

ASAN info:

```
ASAN:SIGSEGV
=================================================================
==17359==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000001 (pc 0x7f2e6f6c3fc6 bp 0x7ffd238e70b0 sp 0x7ffd238e6f00 T0)
    #0 0x7f2e6f6c3fc5 in expand_mmacro  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:4764
    #1 0x7f2e6f6c3fc5 in pp_getline  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:5128
    #2 0x7f2e6f6a9d46 in nasm_preproc_get_line  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-preproc.c:198
    #3 0x7f2e6f69b2ac in nasm_parser_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:218
    #4 0x7f2e6f68f36b in nasm_do_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:66
    #5 0x7f2e6f68f36b in nasm_parser_do_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:83
    #6 0x402c84 in do_assemble  test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:521
    #7 0x402c84 in main  test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:753
    #8 0x7f2e7286b82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #9 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/preprocs/nasm/nasm-pp.c:4764 expand_mmacro
==17359==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