New issue

Jump to bottom

# A NULL pointer dereference in the function yasm_expr_get_intnum() libyasm/expr.c:1263 #166

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` )

I think it is probably a similar issue as #83

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-1377-yasm_expr_get_intnum-null-pointer-deref

ASAN info:

```
yasm: file name already has no extension: output will be in `yasm.out'
ASAN:SIGSEGV
=================================================================
==12603==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f421b49db7e bp 0x7ffc83d244d0 sp 0x7ffc83d244c0 T0)
    #0 0x7f421b49db7d in yasm_expr_get_intnum  test/yasm-uaf/SRC_asan/libyasm/expr.c:1263
    #1 0x7f421b487b9e in bc_align_finalize  test/yasm-uaf/SRC_asan/libyasm/bc-align.c:108
    #2 0x7f421b48c6ee in yasm_bc_finalize  test/yasm-uaf/SRC_asan/libyasm/bytecode.c:176
    #3 0x7f421b4b9bd2 in yasm_object_finalize  test/yasm-uaf/SRC_asan/libyasm/section.c:528
    #4 0x402ca9 in do_assemble  test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:527
    #5 0x402ca9 in main  test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:753
    #6 0x7f421aeba82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #7 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/libyasm/expr.c:1263 yasm_expr_get_intnum
==12603==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