New issue

Jump to bottom

AddressSanitizer: heap-buffer-overflow in inc_fopen() modules/preprocs/nasm/nasm-pp.c:1835 #164

Open **Clingto** opened this issue on May 19, 2021 · 4 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-7306d-inc_fopen-heap-buffer-overflow

ASAN info:

```
yasm: file name already has no extension: output will be in `yasm.out'
=================================================================
==19224==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x603000009cea at pc 0x7f3f6962c06e bp 0x7ffce951a4d0 sp 0x7ffce9519c78
WRITE of size 23 at 0x603000009cea thread T0
    #0 0x7f3f6962c06d in strcat (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x7306d)
    #1 0x7f3f65bb8458 in strcat /usr/include/x86_64-linux-gnu/bits/string3.h:148
    #2 0x7f3f65bb8458 in inc_fopen  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:1835
    #3 0x7f3f65bb8458 in do_directive  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:2737
    #4 0x7f3f65bc0333 in pp_getline  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:5083
    #5 0x7f3f65ba9d46 in nasm_preproc_get_line  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-preproc.c:198
    #6 0x7f3f65b9b2ac in nasm_parser_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:218
    #7 0x7f3f65b8f36b in nasm_do_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:66
    #8 0x7f3f65b8f36b in nasm_parser_do_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:83
    #9 0x402c84 in do_assemble  test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:521
    #10 0x402c84 in main  test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:753
    #11 0x7f3f68d9782f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #12 0x403ee8 in _start ( test/yasm-uaf/bin_asan/bin/yasm+0x403ee8)

0x603000009cea is located 0 bytes to the right of 26-byte region [0x603000009cd0,0x603000009cea)
allocated by thread T0 here:
    #0 0x7f3f69651602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
    #1 0x7f3f693a2769 in def_xmalloc  test/yasm-uaf/SRC_asan/libyasm/xmalloc.c:69
    #2 0x7f3f65bb840c in inc_fopen  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:1823
    #3 0x7f3f65bb840c in do_directive  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:2737
    #4 0x7f3f65bc0333 in pp_getline  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:5083
    #5 0x7f3f65ba9d46 in nasm_preproc_get_line  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-preproc.c:198
    #6 0x7f3f65b9b2ac in nasm_parser_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:218
    #7 0x7f3f65b8f36b in nasm_do_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:66
    #8 0x7f3f65b8f36b in nasm_parser_do_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:83
    #9 0x402c84 in do_assemble  test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:521
    #10 0x402c84 in main  test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:753
    #11 0x7f3f68d9782f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)

SUMMARY: AddressSanitizer: heap-buffer-overflow ??:0 strcat
Shadow bytes around the buggy address:
  0x0c067fff9340: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff9350: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff9360: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff9370: fa fa fa fa fa fa fd fd fd fa fa fa fd fd fd fa
  0x0c067fff9380: fa fa fd fd fd fa fa fa fd fd fd fd fa fa fa fd
=>0x0c067fff9390: fd fa fa fa fd fd fd fa fa fa 00 00 00[02]fa fa
  0x0c067fff93a0: fd fd fd fa fa fa fd fd fd fa fa fa fd fd fd fa
  0x0c067fff93b0: fa fa fd fd fd fa fa fa fd fd fd fa fa fa fd fd
  0x0c067fff93c0: fd fa fa fa fd fd fd fa fa fa fd fd fd fa fa fa
  0x0c067fff93d0: fd fd fd fa fa fa fd fd fd fa fa fa fd fd fd fa
  0x0c067fff93e0: fa fa fd fd fd fa fa fa fd fd fd fa fa fa 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
==19224==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

petterreinholdtsen commented on Aug 4

According to https://security-tracker.debian.org/tracker/CVE-2021-33464, this is a security issue assigned CVE-2021-33464.

bgermann commented 2 days ago

It has been 1.5 years without this CVE fixed. Can somebody please take care of this?

petterreinholdtsen commented 2 days ago

[bgermann]

> It has been 1.5 years without this CVE fixed. Can somebody please take care of this?

Perhaps the maintainer is no more, and a replacement / fork is needed/
...

PeterJohnson commented 2 days ago Member

I'm still alive, but have moved on to other projects. If someone else wants to take on maintainership, I'd be happy to give them the access to this repo do so (presumably with some kind of transitional period where I would review/approve PRs).

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants