



Comments (3) Dependencies Duplicates (0) Blocking (0) Resources (1)

Fixed Bug P3 [AOSP] assigned adexe s nau

DESCRIPTION kd...@gmail.com created issue #1

short description

There is a memcpy-param-overlap in function impeg2_mc_fullx_fully_8x8 in the libmpeg2, can be triggered via mpeg2_dec_fuzzer (oss-fuzz driver) + ASan

A security Bug?

Yes, a denial of service

how to reproduce

Compile the libmpeg2using the instruction with sanitizer, and build corresponding fuzzer, run mpeg2_dec_fuzzer via command ./mpeg2_dec_fuzzer \$POC

ASan output

```
INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 2441881174
INFO: Loaded 1 modules   (84 inline 8-bit counters): 84 [0x64b470, 0x64b4c4),
INFO: Loaded 1 PC tables (84 PCs): 84 [0x6085f0,0x608b30),
./mpeg2_dec_fuzzer: Running 1 inputs 1 time(s) each.
Running: poc0
=====
==156830==ERROR: AddressSanitizer: memcpy-param-overlap: memory ranges [0x7f5d58fe9678,0x7f5d58fe9680) and [0x7f5d58fe9679, 0x7f5d58fe9681) o
#0 0x520c74 in __asan_memcpy (/home/kdsj/workspace/benchmarks/large/libmpeg2/build/mpeg2_dec_fuzzer+0x520c74)
#1 0x5e5d88 in impeg2_mc_fullx_fully_8x8 /home/kdsj/workspace/benchmarks/large/libmpeg2/common/impeg2_inter_pred.c:462:9
#2 0x5df060 in impeg2d_mc_fullx_fully /home/kdsj/workspace/benchmarks/large/libmpeg2/decoder/impeg2d_mc.c:1244:9
#3 0x5d8b8e in impeg2d_motion_comp_recon_buf /home/kdsj/workspace/benchmarks/large/libmpeg2/decoder/impeg2d_mc.c:182:5
#4 0x5d8ffc in impeg2d_mc_lmv /home/kdsj/workspace/benchmarks/large/libmpeg2/decoder/impeg2d_mc.c:229:5
#5 0x582190 in impeg2d_dec_p_b_slice /home/kdsj/workspace/benchmarks/large/libmpeg2/decoder/impeg2d_pnb_pic.c:595:13
#6 0x5caf82 in impeg2d_dec_slice /home/kdsj/workspace/benchmarks/large/libmpeg2/decoder/impeg2d_dec_hdr.c:924:15
#7 0x5cbf04 in impeg2d_dec_pic_data_thread /home/kdsj/workspace/benchmarks/large/libmpeg2/decoder/impeg2d_dec_hdr.c:1040:23
#8 0x5ce989 in impeg2d_dec_pic_data /home/kdsj/workspace/benchmarks/large/libmpeg2/decoder/impeg2d_dec_hdr.c:1522:5
#9 0x5d4148 in impeg2d_process_video_bit_stream /home/kdsj/workspace/benchmarks/large/libmpeg2/decoder/impeg2d_dec_hdr.c:1988:17
#10 0x576c6d in impeg2d_dec_frm /home/kdsj/workspace/benchmarks/large/libmpeg2/decoder/impeg2d_decoder.c:226:19
#11 0x573d0c in impeg2d_api_entity /home/kdsj/workspace/benchmarks/large/libmpeg2/decoder/impeg2d_api_main.c:3570:17
#12 0x564e6b in impeg2d_api_function /home/kdsj/workspace/benchmarks/large/libmpeg2/decoder/impeg2d_api_main.c:1407:25
#13 0x55b23d in Codec::decodeFrame(unsigned char const*, unsigned long, unsigned long*) (/home/kdsj/workspace/benchmarks/large/libmpeg2/b
#14 0x55c498 in LLVMFuzzerTestOneInput (/home/kdsj/workspace/benchmarks/large/libmpeg2/build/mpeg2_dec_fuzzer+0x55c498)
#15 0x456f23 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) fuzzer.o
#16 0x442a62 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) fuzzer.o
#17 0x44898b in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) fuzzer.o
#18 0x471e22 in main (/home/kdsj/workspace/benchmarks/large/libmpeg2/build/mpeg2_dec_fuzzer+0x471e22)
#19 0x7f5d5cb83fcf in __libc_start_call_main csu/../sysdeps/nptl/libc_start_call_main.h:58:16
#20 0x7f5d5cb8407c in __libc_start_main csu/../csu/libc-start.c:409:3
#21 0x41f6d4 in _start (/home/kdsj/workspace/benchmarks/large/libmpeg2/build/mpeg2_dec_fuzzer+0x41f6d4)

0x7f5d58fe9678 is located 8330872 bytes inside of 12585600-byte region [0x7f5d587f7800,0x7f5d593f8280)
allocated by thread T0 here:
#0 0x522427 in __interceptor_posix_memalign (/home/kdsj/workspace/benchmarks/large/libmpeg2/build/mpeg2_dec_fuzzer+0x522427)
#1 0x556e32 in Codec::createCodec() (/home/kdsj/workspace/benchmarks/large/libmpeg2/build/mpeg2_dec_fuzzer+0x556e32)
#2 0x55c2f5 in LLVMFuzzerTestOneInput (/home/kdsj/workspace/benchmarks/large/libmpeg2/build/mpeg2_dec_fuzzer+0x55c2f5)
#3 0x456f23 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) fuzzer.o
#4 0x442a62 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) fuzzer.o
#5 0x44898b in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) fuzzer.o
#6 0x471e22 in main (/home/kdsj/workspace/benchmarks/large/libmpeg2/build/mpeg2_dec_fuzzer+0x471e22)
#7 0x7f5d5cb83fcf in __libc_start_call_main csu/../sysdeps/nptl/libc_start_call_main.h:58:16

0x7f5d58fe9679 is located 8330873 bytes inside of 12585600-byte region [0x7f5d587f7800,0x7f5d593f8280)
allocated by thread T0 here:
#0 0x522427 in __interceptor_posix_memalign (/home/kdsj/workspace/benchmarks/large/libmpeg2/build/mpeg2_dec_fuzzer+0x522427)
#1 0x556e32 in Codec::createCodec() (/home/kdsj/workspace/benchmarks/large/libmpeg2/build/mpeg2_dec_fuzzer+0x556e32)
#2 0x55c2f5 in LLVMFuzzerTestOneInput (/home/kdsj/workspace/benchmarks/large/libmpeg2/build/mpeg2_dec_fuzzer+0x55c2f5)
#3 0x456f23 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) fuzzer.o
#4 0x442a62 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) fuzzer.o
#5 0x44898b in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) fuzzer.o
#6 0x471e22 in main (/home/kdsj/workspace/benchmarks/large/libmpeg2/build/mpeg2_dec_fuzzer+0x471e22)
#7 0x7f5d5cb83fcf in __libc_start_call_main csu/../sysdeps/nptl/libc_start_call_main.h:58:16
```

SUMMARY: AddressSanitizer: memcpy-param-overlap (/home/kdsj/workspace/benchmarks/large/libmpeg2/build/mpeg2_dec_fuzzer+0x520c74) in __asan_me
==156830==ABORTING

what should happen


It should run normally


Environment

Ubuntu 21.10 clang 13.0.0-2 libmpeg latest commit 33be8ea9ce8f051f52240f931644a14e23ccedb4

POC

As shown in the attachment.

 **poc.zip**

4.4 KB Download 


COMMENTS

AI




vi...@google.com <vi...@google.com> [#2](#)
Assigned to vi...@google.com.

We've shared this with our product and engineering teams and will continue to provide updates as more information becomes available.



te...@gmail.com <te...@gmail.com> [#3](#)

FYI, I actually ran into the same issue and made a patch here: <https://android-review.googlesource.com/c/platform/external/libmpeg2/+/-/2132593>



es...@google.com <es...@google.com>
Marked as fixed.