Pwno

Ruikai Peng <ruikai@pwno.io>

Heap OOB write in MPEG-TS JPEG-XS PES parsing (libavformat/mpegts.c) introduced by 536475ea058245e71f5c2e7f3d5c39b0cad465e5

Ruikai Peng <ruikai@pwno.io> Sun, Dec 14, 2025 at 10:14 AM
To: ffmpeg-security@ffmpeg.org

ffmpeg-security team,

I'm reporting a reachable heap out-of-bounds write in the MPEG-TS demuxer's JPEG-XS handling. It is present on current origin/master (b802eeabff59b3c95dd3efc411253db9b1a558f0) and was introduced by commit 536475ea058245e71f5c2e7f3d5c39b0cad465e5 ("avformat/mpegts: add support for JPEG-XS streams").

Vulnerable code (libavformat/mpegts.c:new_pes_packet):

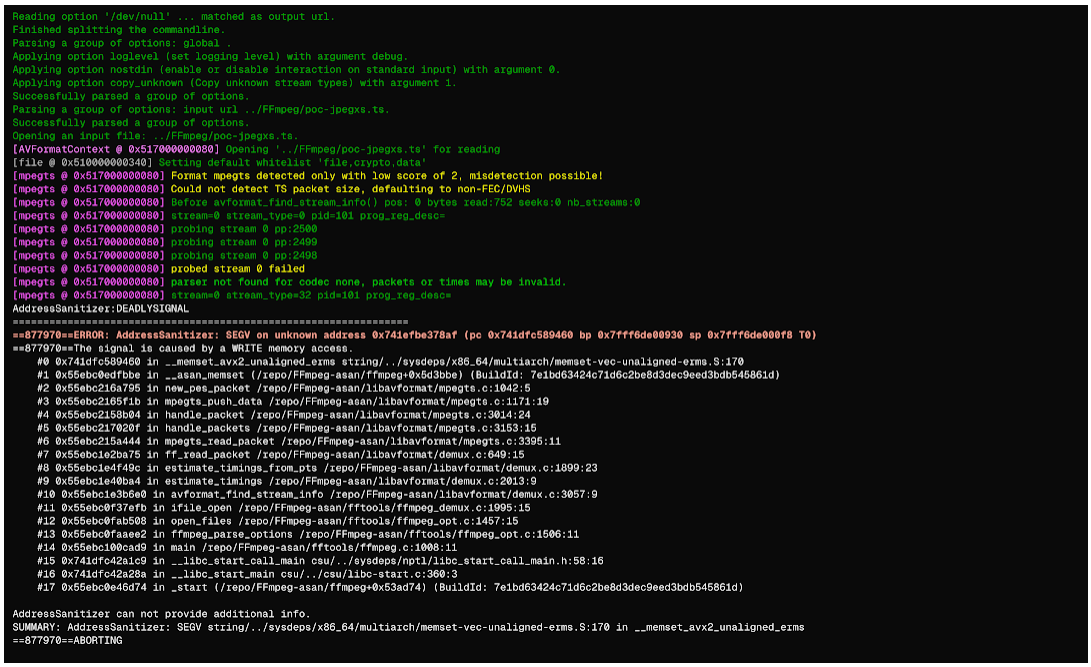
```
// JPEG-XS PES payload
if (pes->stream_id == 0xbd && pes->stream_type == 0x32 &&
    pkt->size >= 8 && memcmp(pkt->data + 4, "jxes", 4) == 0)
{
    uint32_t header_size = AV_RB32(pkt->data);
    pkt->data += header_size;
    pkt->size -= header_size;
}

memset(pkt->data + pkt->size, 0, AV_INPUT_BUFFER_PADDING_SIZE);
```

header_size comes from the PES payload and is never bounds-checked against pkt->size. If header_size > pkt->size, pkt->data is advanced past the buffer and pkt->size underflows/overflows, so the trailing memset writes to an attacker-controlled address, causing a crash (and potentially corruption).

Reproduction (ASan):
- Build with ASan (clang), no special options beyond --enable-debug=3 --disable-optimizations --extra-cflags='-fsanitize=address -fno-omit-frame-pointer' --extra-ldflags='-fsanitize=address'.
- PoC: minimal TS with PAT/PMT (stream_type 0x32) and a PES on PID 0x101 with stream_id = 0xbd, payload starting with AV_RB32 = 0xFFFFFF00 followed by "jxes", then a second PES to flush.
- Command:

```
ASAN_OPTIONS=halt_on_error=1:detect_leaks=0 ./ffmpeg -loglevel debug -nostdin \
  -i poc-jpegxs.ts -copy_unknown -map 0 -c copy -f null /dev/null
```



```
Reading option '/dev/null' ... matched as output url.
Finished splitting the commandline.
Parsing a group of options: global .
Applying option loglevel (set logging level) with argument debug.
Applying option nostdin (enable or disable interaction on standard input) with argument 0.
Applying option copy_unknown (Copy unknown stream types) with argument 1.
Successfully parsed a group of options.
Parsing a group of options: input url ../FFmpeg/poc-jpegxs.ts.
Successfully parsed a group of options.
Opening an input file: ../FFmpeg/poc-jpegxs.ts.
[AVFormatContext @ 0x5170000000080] Opening '../FFmpeg/poc-jpegxs.ts' for reading
[file @ 0x510000000340] Setting default whitelist 'file,crypto,data'
[mpegts @ 0x5170000000080] Format mpegts detected only with low score of 2, misdetection possible!
[mpegts @ 0x5170000000080] Could not detect TS packet size, defaulting to non-FEC/DVHS
[mpegts @ 0x5170000000080] Before avformat_find_stream_info() pos: 0 bytes read:752 seeks:0 nb_streams:0
[mpegts @ 0x5170000000080] stream=0 stream_type=0 pid=101 prog_reg_desc=
[mpegts @ 0x5170000000080] probing stream 0 pp:2500
[mpegts @ 0x5170000000080] probing stream 0 pp:2499
[mpegts @ 0x5170000000080] probing stream 0 pp:2498
[mpegts @ 0x5170000000080] probed stream 0 failed
[mpegts @ 0x5170000000080] parser not found for codec none, packets or times may be invalid.
[mpegts @ 0x5170000000080] stream=0 stream_type=32 pid=101 prog_reg_desc=
AddressSanitizer:DEADLYSIGNAL
=================================================================
==877970==ERROR: AddressSanitizer: SEGV on unknown address 0x741efbe378af (pc 0x741dfc589460 bp 0x7fff6de00930 sp 0x7fff6de000f8 T0)
==877970==The signal is caused by a WRITE memory access.
    #0 0x741dfc589460 in __memset_avx2_unaligned_erms string/../sysdeps/x86_64/multiarch/memset-vec-unaligned-erms.S:170
    #1 0x55ebc0edfbbe in __asan_memset (/repo/FFmpeg-asan/ffmpeg+0x6d3bbe) (BuildId: 7e1bd63424c71d6c2be8d3dec9eed3bdb545861d)
    #2 0x55ebc216a795 in new_pes_packet /repo/FFmpeg-asan/libavformat/mpegts.c:1042:5
    #3 0x55ebc2165f1b in mpegts_push_data /repo/FFmpeg-asan/libavformat/mpegts.c:1171:19
    #4 0x55ebc2158b04 in handle_packet /repo/FFmpeg-asan/libavformat/mpegts.c:3014:24
    #5 0x55ebc217020f in handle_packets /repo/FFmpeg-asan/libavformat/mpegts.c:3153:15
    #6 0x55ebc215a444 in mpegts_read_packet /repo/FFmpeg-asan/libavformat/mpegts.c:3395:11
    #7 0x55ebc1e2ba75 in ff_read_packet /repo/FFmpeg-asan/libavformat/demux.c:649:15
    #8 0x55ebc1e4f49c in estimate_timings_from_pts /repo/FFmpeg-asan/libavformat/demux.c:1899:23
    #9 0x55ebc1e40ba4 in estimate_timings /repo/FFmpeg-asan/libavformat/demux.c:2013:9
    #10 0x55ebc1e3b6e0 in avformat_find_stream_info /repo/FFmpeg-asan/libavformat/demux.c:3057:9
    #11 0x55ebc0f37efb in ifile_open /repo/FFmpeg-asan/fftools/ffmpeg_demux.c:1995:15
    #12 0x55ebc0fab508 in open_files /repo/FFmpeg-asan/fftools/ffmpeg_opt.c:1457:15
    #13 0x55ebc0faaee2 in ffmpeg_parse_options /repo/FFmpeg-asan/fftools/ffmpeg_opt.c:1506:11
    #14 0x55ebc100cad9 in main /repo/FFmpeg-asan/fftools/ffmpeg.c:1008:11
    #15 0x741dffc42a1c9 in __libc_start_call_main csu/../sysdeps/nptl/libc_start_call_main.h:58:16
    #16 0x741dffc42a28a in __libc_start_main csu/../csu/libc-start.c:360:3
    #17 0x55ebc0e46d74 in _start (/repo/FFmpeg-asan/ffmpeg+0x53ad74) (BuildId: 7e1bd63424c71d6c2be8d3dec9eed3bdb545861d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV string/../sysdeps/x86_64/multiarch/memset-vec-unaligned-erms.S:170 in __memset_avx2_unaligned_erms
==877970==ABORTING
```

- ASan result: SIGSEGV in __asan_memset from new_pes_packet at libavformat/mpegts.c:1042. Backtrace shows new_pes_packet -> mpegts_push_data -> handle_packet -> mpegts_read_packet -> avformat_find_stream_info.

Root cause: missing bounds check on header_size before adjusting pkt->data/pkt->size. A simple fix would be to reject/mark corrupt when header_size > pkt->size (or header_size > pkt->size - AV_INPUT_BUFFER_PADDING_SIZE) before pointer/size adjustment.

I will write a patch

Thanks,
- Ruikai Peng