



Ruikai Peng <ruikai@pwno.io>

Crash in vf_noise SSE2 on misaligned frames (commit 3ba570de8b666f5ae274b99d33cf4d4628cc385b)

Ruikai Peng <ruikai@pwno.io>

Mon, Dec 8, 2025 at 12:57 AM

To: ffmpeg-security@ffmpeg.org

Hi ffmpeg-security team,

I'm reporting a crash in the noise filter introduced in commit 3ba570de8b666f5ae274b99d33cf4d4628cc385b (port from MMX to SSE2). The SSE2 inline asm in libavfilter/x86/vf_noise.c (line_noise_sse2 and line_noise_avg_sse2) uses aligned loads/stores (movdqa, movntdq) but never checks pointer alignment. When the filter reuses an input frame (common path when av_frame_is_writable() is true), it may receive misaligned data from upstream filters that adjust frame->data[i] in place, notably vf_crop:

- vf_crop adjusts plane pointers by arbitrary byte offsets (frame->data[plane] += ...), so an x offset of 1 on 8-bit formats produces a 1-byte misalignment.
- The noise filter then calls the SSE2 path directly on those pointers without realigning or falling back.

Repro on x86_64/SSE2 (current HEAD at that commit):

```
./ffmpeg -v error -f lavfi -i testsrc=s=320x240:rate=1 \
-vf "format=yuv420p,crop=w=319:x=1:h=240:exact=1,noise=all=50" \
-frames:v 1 -f null -
```

```
zetr@factory: /tmp/ffmpeg$ ASAN_OPTIONS="abort_on_error=1:disable_coredump=0:strict_string_checks=1:detect_leaks=0" ./ffmpeg -v error -f lavfi -i testsrc=s=320x240:rate=1
-vf "format=yuv420p,crop=w=319:x=1:h=240:exact=1,noise=all=50" -frames:v 1 -f null -
AddressSanitizerAddressSanitizerAddressSanitizerAddressSanitizerAddressSanitizerAddressSanitizerAddressSanitizer:DEADLYSIGNAL
:DEADLYSIGNAL
:DEADLYSIGNAL
:DEADLYSIGNAL
:DEADLYSIGNAL
:DEADLYSIGNAL
:DEADLYSIGNAL
=====
AddressSanitizer:DEADLYSIGNAL
==56849==ERROR: AddressSanitizer: SEGV on unknown address (pc 0x635cf13a9720 bp 0x730256172d00 sp 0x730256172c18 T15)
AddressSanitizer:DEADLYSIGNAL
==56849==The signal is caused by a READ memory access.
==56849==Hint: this fault was caused by a dereference of a high value address (see register values below). Disassemble the provided pc to learn which register was used.
#0 0x635cf13a9720 in line_noise_sse2 libavfilter/x86/vf_noise.c:84
#1 0x635cf1154216 in noise libavfilter/vf_noise.c:218
#2 0x635cf1154216 in filter_slice libavfilter/vf_noise.c:236
#3 0x635cf0e5fc81 in worker_func libavfilter/pthread.c:48
#4 0x635cf3bc33a3 in run_jobs libavutil/slicethread.c:65
#5 0x635cf3bc33a3 in thread_worker libavutil/slicethread.c:89
#6 0x770269a3f002 in asan_thread_start ../../../../src/libasanitizer/asan/asan_interceptors.cpp:239
#7 0x770269a3d83 in start_thread nptl/ptthread_create.c:448
#8 0x7702699373bb in __clone3 ../../sysdeps/unix/sysv/linux/x86_64/clone3.S:78

==56849==Register values:
rax = 0xfffffffffffffed0 rdx = 0x0000000000000005 icx = 0x000000000000013f idx = 0x00007522589ef46c
r11 = 0x00007612689e4b71 r12 = 0xfffffffffffffed0 rbp = 0x0000730256172d00 r10 = 0x0000736256172c18
r13 = 0x000000000000036c r9 = 0x00007612689e4b71 r10 = 0x0000000000000130 r11 = 0x0000745268a86240
r12 = 0x0000000000000100 r13 = 0x0000000000000007 r14 = 0x0000770268b37800 r15 = 0x000000000000013f
AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV libavfilter/x86/vf_noise.c:84 in line_noise_sse2
Thread T15 created by T10 (vfork@0) here:
#0 0x770269d196aa in pthread_create ../../../../src/libasanitizer/asan/asan_interceptors.cpp:250
#1 0x635cf0cbf053 in avpriv_slicethread_create libavutil/slicethread.c:174
#2 0x635cf0e5febd in thread_init_internal libavfilter/pthread.c:76
#3 0x635cf0e5febd in ff_graph_thread_init libavfilter/pthread.c:96
#4 0x635cf0e18bcf in avfilter_graph_alloc_filter libavfilter/avfiltergraph.c:178
#5 0x635cf0e0a3b3 in avfilter_graph_segment_create_filters libavfilter/graphparser.c:553
#6 0x635cf0e0a3b3 in avfilter_graph_segment_create_filters libavfilter/graphparser.c:516
#7 0x635cf0d1c0c5 in graph_parse_fftools/ffmpeg_filter.c:575
#8 0x635cf0d28048 in configure_filtergraph fftools/ffmpeg_filter.c:1976
#9 0x635cf0d2b0c0 in send_frame fftools/ffmpeg_filter.c:2997
#10 0x635cf0d2b0c0 in filter_thread fftools/ffmpeg_filter.c:3156
#11 0x635cf0d5ca42 in task_wrapper fftools/ffmpeg_filter.c:2683
#12 0x770269d5f802 in asan_thread_start ../../../../src/libasanitizer/asan/asan_interceptors.cpp:239
#13 0x770269a3d83 in start_thread nptl/ptthread_create.c:448
```

This crashes with SIGSEGV at the aligned load in line_noise_sse2 (movdqa (%r9,%rax),%xmm0; effective address misaligned by 1 byte).

Impact: denial of service via crafted filtergraphs (e.g., crop + noise). Applies to planar 8-bit formats where upstream filters can shift data pointers without reallocating.

Here's a patch that we have validated, that fixes this issue, please reference the attachment.

Best,
Pwno OSS Team

 **patch.diff**
3K