Pwno

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

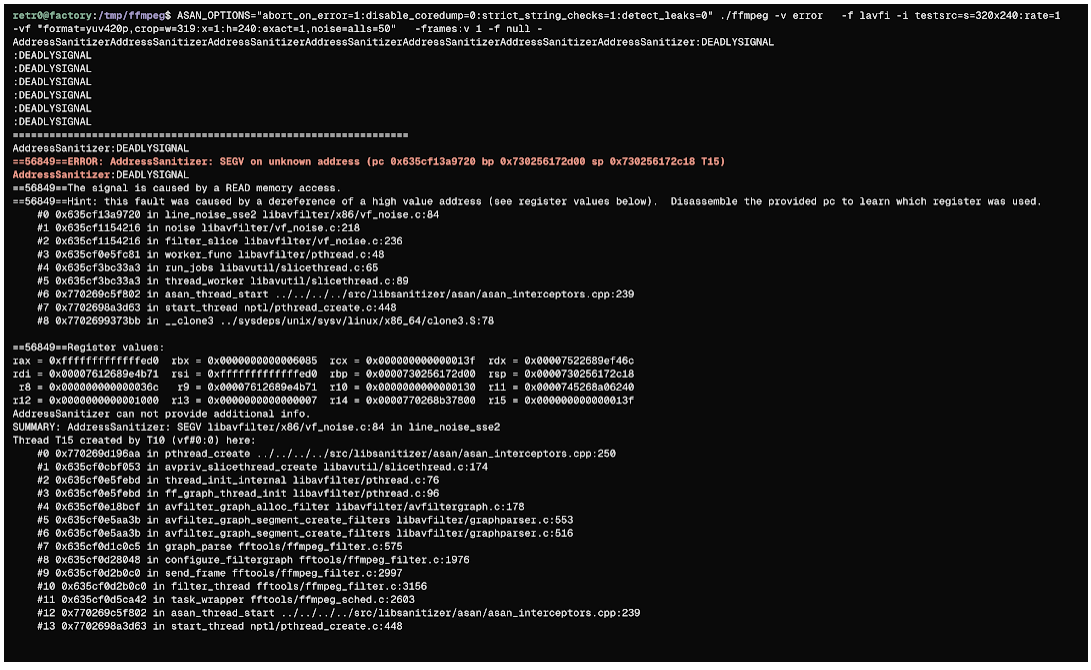
Hi ffmpeg-security team,

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=alls=50" \
-frames:v 1 -f null -



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