Ruikai Peng <ruikai@pwno.io>

Heap Overflow in extended TRC (Panasonic V-Log)

Ruikai Peng <ruikai@pwno.io>
To: ffmpeg-security@ffmpeg.org

Tue, Dec 9, 2025 at 11:29 PM

Hi ffmpeg-security team,

I'm here to report a heap-overflow *(specifically a 237*8 = 1896 bytes heap OOB read)* at ICC profile generation for extended TRC values. Introduced by commit aeb9b19ebc0295d7fcaa5ed09f9b267fea57895c ("lavu: add support for Panasonic V-Log").

Specifically in libavcodec/fflcms2.h, FFIccContext allocates:
*cmsToneCurve *curves[AVCOL_TRC_NB];*
where *AVCOL_TRC_NB* is 19.

Commit aeb9b19... extends the TRC enum for values like AVCOL_TRC_V_LOG = 256
and changes get_curve()'s range check in libavcodec/fflcms2.c:

```
static int get_curve(FFIccContext *s, enum AVColorTransferCharacteristic trc,cmsToneCurve **out_curve)
{
  if ((trc >= AVCOL_TRC_NB && trc < AVCOL_TRC_EXT_BASE) || trc >= AVCOL_TRC_EXT_NB)
    return AVERROR_INVALIDDATA;

  if (s->curves[trc])
    return 0;
```

For trc = AVCOL_TRC_V_LOG (256), the condition allows the value to pass the
range check, but then uses it as an index into s->curves[], which only has
AVCOL_TRC_NB (19) entries. This results in s->curves[256] being read, causing
a heap-buffer-overflow before the later switch statement that treats V-Log
as AVERROR_PATCHWELCOME is reached.

So the path is roughly:
setparams(color_trc=vlog) -> frame->color_trc = 256 -> iccgen -> ff_icc_profile_generate() -> get_curve() -> s->curves[256] (heap OOB access)

- Repro (built with clang + ASan, lcms2 enabled, commit aeb9b19e):

```
ASAN_OPTIONS=detect_leaks=0 ./ffmpeg -v error -f lavfi -i testsrc2=size=16x16:rate=1 \
-frames:v 1 -vf "setparams=color_trc=vlog,iccgen" -f null -
```

```
=================================================================
==98371==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6fd4b29ed458 at pc 0x63a604f05adc bp 0x6eb4a6bad610 sp 0x6eb4a6bad608
READ of size 8 at 0x6fd4b29ed458 thread T10 (vf#0:0)
    #0 0x63a604f05adb in get_curve /repo/ffmpeg-asan/./libavcodec/fflcms2.c:56:9
    #1 0x63a604f05297 in ff_icc_profile_generate /repo/ffmpeg-asan/./libavcodec/fflcms2.c:157:16
    #2 0x63a6049b3837 in iccgen_filter_frame /repo/ffmpeg-asan/libavfilter/vf_iccgen.c:145:20
    #3 0x63a6046f125d in filter_frame_framed /repo/ffmpeg-asan/libavfilter/avfilter.c:1058:11
    #4 0x63a6046f125d in filter_frame_to_filter /repo/ffmpeg-asan/libavfilter/avfilter.c:1214:11
    #5 0x63a6046f125d in filter_activate_default /repo/ffmpeg-asan/libavfilter/avfilter.c:1276:20
    #6 0x63a6046f125d in ff_filter_activate /repo/ffmpeg-asan/libavfilter/avfilter.c:1458:49
    #7 0x63a604709577 in push_frame /repo/ffmpeg-asan/libavfilter/buffersrc.c:200:15
    #8 0x63a604709577 in av_buffersrc_add_frame_flags /repo/ffmpeg-asan/libavfilter/buffersrc.c:272:15
    #9 0x63a6045ede6f in send_frame /repo/ffmpeg-asan/fftools/ffmpeg_filter.c:3016:11
    #10 0x63a6045ede6f in filter_thread /repo/ffmpeg-asan/fftools/ffmpeg_filter.c:3156:19
    #11 0x63a60462ca99 in task_wrapper /repo/ffmpeg-asan/fftools/ffmpeg_sched.c:2603:11
    #12 0x63a60458396a in asan_thread_start(void*) asan_interceptors.cpp.o
    #13 0x72b4b3aa3d63 in start_thread nptl/pthread_create.c:448:8
    #14 0x72b4b3b373bb in __GI___clone3 misc/../sysdeps/unix/sysv/linux/x86_64/clone3.S:78

0x6fd4b29ed458 is located 1440 bytes after 248-byte region [0x6fd4b29ecdc0,0x6fd4b29eceb8)
allocated by thread T10 (vf#0:0) here:
    #0 0x63a604586b3b in posix_memalign (/repo/ffmpeg-asan/ffmpeg+0x77db3b) (BuildId: 939a4a63401f198017709fbf7917850116bb12a3)
    #1 0x63a607ba5a7c in av_malloc /repo/ffmpeg-asan/libavutil/mem.c:107:9
    #2 0x63a607ba5a7c in av_mallocz /repo/ffmpeg-asan/libavutil/mem.c:258:17
    #3 0x63a6046ed4bb in ff_filter_alloc /repo/ffmpeg-asan/libavfilter/avfilter.c:720:25
    #4 0x63a6046f577c in avfilter_graph_alloc_filter /repo/ffmpeg-asan/libavfilter/avfiltergraph.c:191:9
    #5 0x63a6046f5547 in avfilter_graph_create_filter /repo/ffmpeg-asan/libavfilter/avfiltergraph.c:146:17
    #6 0x63a6045f4090 in configure_output_video_filter /repo/ffmpeg-asan/fftools/ffmpeg_filter.c:1534:11
    #7 0x63a6045f4090 in configure_output_filter /repo/ffmpeg-asan/fftools/ffmpeg_filter.c:1689:37
    #8 0x63a6045f4090 in configure_filtergraph /repo/ffmpeg-asan/fftools/ffmpeg_filter.c:1989:15
    #9 0x63a6045edcac in send_frame /repo/ffmpeg-asan/fftools/ffmpeg_filter.c:2997:15
    #10 0x63a6045edcac in filter_thread /repo/ffmpeg-asan/fftools/ffmpeg_filter.c:3156:19
    #11 0x63a60462ca99 in task_wrapper /repo/ffmpeg-asan/fftools/ffmpeg_sched.c:2603:11
    #12 0x63a60458396a in asan_thread_start(void*) asan_interceptors.cpp.o

Thread T10 (vf#0:0) created by T0 here:
    #0 0x63a60456a165 in pthread_create (/repo/ffmpeg-asan/ffmpeg+0x761165) (BuildId: 939a4a63401f198017709fbf7917850116bb12a3)
    #1 0x63a60462609b in task_start /repo/ffmpeg-asan/fftools/ffmpeg_sched.c:412:11
    #2 0x63a604625506 in sch_start /repo/ffmpeg-asan/fftools/ffmpeg_sched.c:1666:15
    #3 0x63a60465c8ff in transcode /repo/ffmpeg-asan/fftools/ffmpeg.c:879:11
    #4 0x63a60465c8ff in main /repo/ffmpeg-asan/fftools/ffmpeg.c:1010:11
    #5 0x72b4b3a2a574 in __libc_start_call_main csu/../sysdeps/nptl/libc_start_call_main.h:58:16
    #6 0x72b4b3a2a627 in __libc_start_main csu/../csu/libc-start.c:360:3
    #7 0x63a6044e2534 in _start (/repo/ffmpeg-asan/ffmpeg+0x6d9534) (BuildId: 939a4a63401f198017709fbf7917850116bb12a3)

SUMMARY: AddressSanitizer: heap-buffer-overflow /repo/ffmpeg-asan/./libavcodec/fflcms2.c:56:9 in get_curve
Shadow bytes around the buggy address:
  0x6fd4b29ed180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

- ASan: heap-buffer-overflow at libavcodec/fflcms2.c:56 in get_curve, reading s->curves[256].
- Reachability: vf_setparams allows color_trc=vlog (value 256). vf_iccgen and encoder ICC generation call ff_icc_profile_generate(), which calls get_curve() and performs the OOB read before the switch returns AVERROR_PATCHWELCOME.

I am working on a patch at the moment, since it's 11 p.m. here at ET, I'll try my best to provide a .diff today, at the meantime, I recommend either reject extended TRCs before indexing or extend the cache *(e.g., separate curves_ext array indexed by trc - AVCOL_TRC_EXT_BASE)*

Best,
Ruikai Peng
Pwno OSS Team