#8276 closed defect (fixed)

Opened 3 years ago
Closed 3 years ago

heap-buffer-overflow at libavfilter/af_afade.c:436:1 in crossfade_samples_fltp

Reported by:	Suhwan	Owned by:	
Priority:	normal	Component:	undetermined
Version:	git-master	Keywords:	asan
Cc:		Blocked By:	
Blocking:		Reproduced by developer:	no
Analyzed by developer:	no		

Description

Summary of the bug:
There is a heap-buffer-overflow at libavfilter/af_afade.c:436:1 in crossfade_samples_fltp

I compiled ffmpeg with "--toolchain=clang-asan" to check the memory corruption and attached log file.
How to reproduce:

```
% ffmpeg_g -y -i $PoC1 -i $PoC2 -filter_complex acrossfade tmp.tta

ffmpeg version N-95382-g62f4722582 Copyright (c) 2000-2019 the FFmpeg developers
built with clang version 6.0.0-1ubuntu2 (tags/RELEASE_600/final)
configuration: --cc=clang --cxx=clang++ --ld=clang --enable-debug --toolchain=clan
```

Here's ASAN log

```
==30297==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7fffd8445800 a
READ of size 4 at 0x7fffd8445800 thread T0
    #0 0x16a73a1 in crossfade_samples_fltp ffmpeg/libavfilter/af_afade.c:436:1
    #1 0x169963c in activate ffmpeg/libavfilter/af_afade.c:504:13
    #2 0x824c3e in ff_filter_activate ffmpeg/libavfilter/avfilter.c:1442:38
    #3 0x8700b2 in push_frame ffmpeg/libavfilter/buffersrc.c:187:15
    #4 0x8700b2 in av_buffersrc_add_frame_internal ffmpeg/libavfilter/buffersrc.c:
    #5 0x86eaf2 in av_buffersrc_add_frame_flags ffmpeg/libavfilter/buffersrc.c:170
    #6 0x666407 in ifilter_send_frame ffmpeg/fftools/ffmpeg.c:2186:11
    #7 0x666407 in send_frame_to_filters ffmpeg/fftools/ffmpeg.c:2260
    #8 0x605543 in decode_audio ffmpeg/fftools/ffmpeg.c:2327:11
    #9 0x605543 in process_input_packet ffmpeg/fftools/ffmpeg.c:2609
    #10 0x64a707 in process_input ffmpeg/fftools/ffmpeg.c:4508:5
    #11 0x5e7157 in transcode_step ffmpeg/fftools/ffmpeg.c:4628:11
    #12 0x5e7157 in transcode ffmpeg/fftools/ffmpeg.c:4682
    #13 0x5db65b in main ffmpeg/fftools/ffmpeg.c:4884:9
    #14 0x7ffff5c93b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../
    #15 0x41def9 in _start (ffmpeg_asan+0x41def9)

0x7fffd8445800 is located 0 bytes to the right of 159744-byte region [0x7fffd841e8
allocated by thread T0 here:
    #0 0x4de9e8 in posix_memalign (ffmpeg_asan+0x4de9e8)
    #1 0x85924d1 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x84f927d in av_buffer_alloc ffmpeg/libavutil/buffer.c:72:12
    #3 0x84fdc26 in pool_alloc_buffer ffmpeg/libavutil/buffer.c:313:26
    #4 0x84fdc26 in av_buffer_pool_get ffmpeg/libavutil/buffer.c:349
    #5 0x91c368 in ff_frame_pool_get ffmpeg/libavfilter/framepool.c:261:29
    #6 0x6e2d4c in ff_default_get_audio_buffer ffmpeg/libavfilter/audio.c:73:13
    #7 0x82a406 in ff_inlink_consume_samples ffmpeg/libavfilter/avfilter.c:1181:11
    #8 0x1699080 in activate ffmpeg/libavfilter/af_afade.c:492:19
    #9 0x824c3e in ff_filter_activate ffmpeg/libavfilter/avfilter.c:1442:38
    #10 0x8700b2 in push_frame ffmpeg/libavfilter/buffersrc.c:187:15
    #11 0x8700b2 in av_buffersrc_add_frame_internal ffmpeg/libavfilter/buffersrc.c
    #12 0x86eaf2 in av_buffersrc_add_frame_flags ffmpeg/libavfilter/buffersrc.c:17
    #13 0x666407 in ifilter_send_frame ffmpeg/fftools/ffmpeg.c:2186:11
    #14 0x666407 in send_frame_to_filters ffmpeg/fftools/ffmpeg.c:2260
    #15 0x605543 in decode_audio ffmpeg/fftools/ffmpeg.c:2327:11
    #16 0x605543 in process_input_packet ffmpeg/fftools/ffmpeg.c:2609
    #17 0x64a707 in process_input ffmpeg/fftools/ffmpeg.c:4508:5
    #18 0x5e7157 in transcode_step ffmpeg/fftools/ffmpeg.c:4628:11
    #19 0x5e7157 in transcode ffmpeg/fftools/ffmpeg.c:4682
    #20 0x5db65b in main ffmpeg/fftools/ffmpeg.c:4884:9
    #21 0x7ffff5c93b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../

SUMMARY: AddressSanitizer: heap-buffer-overflow ffmpeg/libavfilter/af_afade.c:436:
Shadow bytes around the buggy address:
  0x10007b080ab0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007b080ac0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007b080ad0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007b080ae0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007b080af0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x10007b080b00:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x10007b080b10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x10007b080b20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x10007b080b30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x10007b080b40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x10007b080b50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==30297==ABORTING
```

Please confirm.
Thanks

Attachments (2)

- PoC1_af_afade_436.vob(1.0 MB) - added by Suhwan 3 years ago.
  poc1
- PoC2_af_afade_436.wav(125.0 KB) - added by Suhwan 3 years ago.

poc2

Change History (3)

by Suhwan, 3 years ago

Attachment: *PoC1_af_afade_436.vob* added

poc1

by Suhwan, 3 years ago

Attachment: *PoC2_af_afade_436.wav* added

poc2

comment:1 by Elon Musk, 3 years ago

Resolution: → fixed
Status: new → closed

Note: See TracTickets for help on using tickets.