Opened 3 years ago
Closed 3 years ago

#8317 closed defect (fixed)

heap-buffer-overflow at libavfilter/af_tremolo.c:135

Reported by:	Suhwan	Owned by:	
Priority:	important	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_tremolo.c:135 in config_input()

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

```
% ffmpeg_g -y -i $PoC_1 -i $PoC_2 -filter_complex tremolo -target dv  tmp.vividas

ffmpeg version N-95464-g7056ddc0e0 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

```
=================================================================
==20332==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x629000004770 a
WRITE of size 8 at 0x629000004770 thread T0
    #0 0x1a389f7 in config_input ffmpeg/libavfilter/af_tremolo.c:135:21
    #1 0x812da0 in avfilter_config_links ffmpeg/libavfilter/avfilter.c:369:28
    #2 0x811dae in avfilter_config_links ffmpeg/libavfilter/avfilter.c:307:24
    #3 0x811dae in avfilter_config_links ffmpeg/libavfilter/avfilter.c:307:24
    #4 0x811dae in avfilter_config_links ffmpeg/libavfilter/avfilter.c:307:24
    #5 0x839be2 in graph_config_links ffmpeg/libavfilter/avfiltergraph.c:261:24
    #6 0x839be2 in avfilter_graph_config ffmpeg/libavfilter/avfiltergraph.c:1279
    #7 0x598d73 in configure_filtergraph ffmpeg/fftools/ffmpeg_filter.c:1109:16
    #8 0x6662d7 in ifilter_send_frame ffmpeg/fftools/ffmpeg.c:2179:15
    #9 0x6662d7 in send_frame_to_filters ffmpeg/fftools/ffmpeg.c:2260
    #10 0x6055a3 in decode_audio ffmpeg/fftools/ffmpeg.c:2327:11
    #11 0x6055a3 in process_input_packet ffmpeg/fftools/ffmpeg.c:2609
    #12 0x64a767 in process_input ffmpeg/fftools/ffmpeg.c:4508:5
    #13 0x5e71b7 in transcode_step ffmpeg/fftools/ffmpeg.c:4628:11
    #14 0x5e71b7 in transcode ffmpeg/fftools/ffmpeg.c:4682
    #15 0x5db6bb in main ffmpeg/fftools/ffmpeg.c:4884:9
    #16 0x7feb27859b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../
    #17 0x41def9 in _start (ffmpeg_g+0x41def9)

0x629000004770 is located 0 bytes to the right of 17776-byte region [0x62900000020
allocated by thread T0 here:
    #0 0x4de9e8 in posix_memalign (ffmpeg_g+0x4de9e8)
    #1 0x85c6559 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x85c6559 in av_malloc_array ffmpeg/libavutil/mem.c:188
    #3 0x1a382ff in config_input ffmpeg/libavfilter/af_tremolo.c:128:16

SUMMARY: AddressSanitizer: heap-buffer-overflow ffmpeg/libavfilter/af_tremolo.c:13
Shadow bytes around the buggy address:
  0x0c527fff8890: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c527fff88a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c527fff88b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c527fff88c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c527fff88d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c527fff88e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00[fa]fa
  0x0c527fff88f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c527fff8900: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c527fff8910: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c527fff8920: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c527fff8930: 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
==20332==ABORTING
```

Please confirm.
Thanks

Attachments (2)

- PoC_1(161 bytes) - added by Suhwan 3 years ago.
  poc1
- PoC_2.VOC(34.0 KB) - added by Suhwan 3 years ago.
  poc2

Change History (3)

by Suhwan, 3 years ago

Attachment: *PoC_1*added

poc1

by Suhwan, 3 years ago

Attachment: *PoC_2.VOC*added

poc2

comment:1 by Elon Musk, 3 years ago

Resolution: → fixed
Status: new → closed

Fixed in 58bb9d3a3a6ede1c6cfb82bf671a5f138e6b2144

Note: See TracTickets for help on using tickets.