#8236 closed defect (fixed)

Opened 3 years ago
Closed 3 years ago
Last modified 3 years ago

heap-buffer-overflow at libavfilter/vf_floodfill.c

Reported by:	Suhwan	Owned by:	
Priority:	normal	Component:	avfilter
Version:	git-master	Keywords:	asan floodfill
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/vf_floodfill.c:333:45

```
==48454==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x63000000e500 a
WRITE of size 2 at 0x63000000e500 thread T0
    #0 0x2605a3b in filter_frame ffmpeg/libavfilter/vf_floodfill.c:333:45
    #1 0x113d8c8 in ff_filter_activate_default ffmpeg/libavfilter/avfilter.c:1071:
    #2 0x113d8c8 in ff_filter_activate ffmpeg/libavfilter/avfilter.c:1430
    #3 0x125d263 in push_frame ffmpeg/libavfilter/buffersrc.c:187:15
    #4 0x125d263 in av_buffersrc_add_frame_internal ffmpeg/libavfilter/buffersrc.c
    #5 0x1257ecc in av_buffersrc_add_frame_flags ffmpeg/libavfilter/buffersrc.c:17
    #6 0xa427a8 in ifilter_send_frame ffmpeg/fftools/ffmpeg.c:2196:11
    #7 0xa427a8 in send_frame_to_filters ffmpeg/fftools/ffmpeg.c:2270
    #8 0x8c4e27 in decode_video ffmpeg/fftools/ffmpeg.c:2469:11
    #9 0x8c4e27 in process_input_packet ffmpeg/fftools/ffmpeg.c:2623
    #10 0x9d5063 in process_input ffmpeg/fftools/ffmpeg.c:4518:5
    #11 0x847996 in transcode_step ffmpeg/fftools/ffmpeg.c:4638:11
    #12 0x847996 in transcode ffmpeg/fftools/ffmpeg.c:4692
    #13 0x81cf5f in main ffmpeg/fftools/ffmpeg.c:4894:9
    #14 0x7fd5916a6b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../
    #15 0x41def9 in _start (ffmpeg_usan+0x41def9)

0x63000000e500 is located 0 bytes to the right of 57600-byte region [0x63000000040
allocated by thread T0 here:
    #0 0x4de9e8 in posix_memalign (ffmpeg_usan+0x4de9e8)
    #1 0x1fd86a19 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x1fd86a19 in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x1fd86a19 in av_calloc ffmpeg/libavutil/mem.c:248
    #4 0x2608e4c in config_input ffmpeg/libavfilter/vf_floodfill.c:272:17

SUMMARY: AddressSanitizer: heap-buffer-overflow ffmpeg/libavfilter/vf_floodfill.c:
```

How to reproduce:

```
% ffmpeg_g -stream_loop 5 -y -i $PoC -filter_complex floodfill -target dvd -loglev

ffmpeg version N-95291-g5345965b3f 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
```

Attachments (2)

- gdb-vf_floodfill333(26.2 KB) - added by Suhwan 3 years ago.
- PoC_vf_floodfill333.dpx(22.1 KB) - added by Suhwan 3 years ago.
  poc

Change History (5)

by Suhwan, 3 years ago

Attachment: *gdb-vf_floodfill333*added

by Suhwan, 3 years ago

Attachment: *PoC_vf_floodfill333.dpx*added

poc

comment:1 by Elon Musk, 3 years ago

Resolution: → fixed
Status: new → closed

comment:2 by James, 3 years ago

Component: undetermined → avfilter

Fixed in 1331e001796c656a4a3c770a16121c15ec1db2ac

comment:3 by Carl Eugen Hoyos, 3 years ago

Keywords: floodfill added

Note: See TracTickets for help on using tickets.