Opened 3 years ago
Closed 3 years ago

#8239 closed defect (fixed)

heap-buffer-overflow at libavfilter/vf_fieldmatch.c

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/vf_fieldmatch.c:435 in build_diff_map

I compiled ffmpeg with "--toolchain=clang-asan" to check the heap buffer overflow and attached log file.

Here's ASAN log

```
==43147==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x621000001130 a
READ of size 1 at 0x621000001130 thread T0
    #0 0x25816cb in build_diff_map ffmpeg/libavfilter/vf_fieldmatch.c:435:30
    #1 0x255ee72 in compare_fields ffmpeg/libavfilter/vf_fieldmatch.c:542:13
    #2 0x25171b6 in filter_frame ffmpeg/libavfilter/vf_fieldmatch.c:745:13
    #3 0x24fdb56 in activate ffmpeg/libavfilter/vf_fieldmatch.c:846:15
    #4 0x11348be in ff_filter_activate ffmpeg/libavfilter/avfilter.c:1429:38
    #5 0x125d263 in push_frame ffmpeg/libavfilter/buffersrc.c:187:15
    #6 0x125d263 in av_buffersrc_add_frame_internal ffmpeg/libavfilter/buffersrc.c
    #7 0x1257ecc in av_buffersrc_add_frame_flags ffmpeg/libavfilter/buffersrc.c:17
    #8 0xa427a8 in ifilter_send_frame ffmpeg/fftools/ffmpeg.c:2196:11
    #9 0xa427a8 in send_frame_to_filters ffmpeg/fftools/ffmpeg.c:2270
    #10 0x8c4e27 in decode_video ffmpeg/fftools/ffmpeg.c:2469:11
    #11 0x8c4e27 in process_input_packet ffmpeg/fftools/ffmpeg.c:2623
    #12 0x9d5063 in process_input ffmpeg/fftools/ffmpeg.c:4518:5
    #13 0x847996 in transcode_step ffmpeg/fftools/ffmpeg.c:4638:11
    #14 0x847996 in transcode ffmpeg/fftools/ffmpeg.c:4692
    #15 0x81cf5f in main ffmpeg/fftools/ffmpeg.c:4894:9
    #16 0x7ff771f61b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../
    #17 0x41def9 in _start (ffmpeg_usan+0x41def9)

0x621000001130 is located 0 bytes to the right of 4144-byte region [0x621000000100
allocated by thread T0 here:
    #0 0x4de9e8 in posix_memalign (ffmpeg_usan+0x4de9e8)
    #1 0x1fd801e7 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x250ad60 in config_input ffmpeg/libavfilter/vf_fieldmatch.c:953:19

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

How to reproduce:

```
% ffmpeg_g -t 2 -y -r 41 -i $PoC -filter_complex fieldmatch -loglevel 99 -vframes

ffmpeg version N-95314-g1331e00179 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
```

Please confirm.
Thanks

Attachments (2)

- gdb_vf_fieldmatch_435(34.8 KB) - added by Suhwan 3 years ago.
- PoC_vf_fieldmatch_435.avi(497.6 KB) - added by Suhwan 3 years ago.
  poc

Change History (3)

by Suhwan, 3 years ago

Attachment: *gdb_vf_fieldmatch_435*added

by Suhwan, 3 years ago

Attachment: *PoC_vf_fieldmatch_435.avi*added

poc

comment:1 by Elon Musk, 3 years ago

Resolution: → fixed
Status: new → closed

Fixed in ce5274c1385d55892a692998923802023526b765

Note: See TracTickets for help on using tickets.