#8240 closed defect (fixed)

Opened 3 years ago
Closed 19 months ago

heap-buffer-overflow at libavfilter/vf_yadif.c

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

Description

Summary of the bug:
There is a heap-buffer-overflow at libavfilter/vf_yadif.c:138 in filter_edges

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

How to reproduce:

```
% ffmpeg_g -t 0 -y -r 87 -i $PoC -filter_complex yadif -target dvd -loglevel 0 -ma

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
```

Here's ASAN log

```
==32056==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61a00000fc7f a
READ of size 1 at 0x61a00000fc7f thread T18
    #0 0x458369f in filter_edges ffmpeg/libavfilter/vf_yadif.c:138:5
    #1 0x458d5b7 in filter_slice ffmpeg/libavfilter/vf_yadif.c:217:13
    #2 0x159e267 in worker_func ffmpeg/libavfilter/pthread.c:50:15
    #3 0x2011cbf9 in run_jobs ffmpeg/libavutil/slicethread.c:61:9
    #4 0x201134fd in thread_worker ffmpeg/libavutil/slicethread.c:85:13
    #5 0x4eb9de in __asan::AsanThread::ThreadStart(unsigned long, __sanitizer::ato
    #6 0x7fe17dd4b6da in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x76d
    #7 0x7fe17d45088e in clone /build/glibc-OTsEL5/glibc-2.27/misc/../sysdeps/unix

0x61a00000fc7f is located 1 bytes to the left of 1103-byte region [0x61a00000fc80,
allocated by thread T1 here:
    #0 0x4de9e8 in posix_memalign (ffmpeg_g+0x4de9e8)
    #1 0x1fd8c0b7 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x1fb2ded1 in av_buffer_alloc ffmpeg/libavutil/buffer.c:72:12
    #3 0x1fb2ded1 in av_buffer_allocz ffmpeg/libavutil/buffer.c:85
    #4 0x1fb3f521 in pool_alloc_buffer ffmpeg/libavutil/buffer.c:313:26
    #5 0x1fb3f521 in av_buffer_pool_get ffmpeg/libavutil/buffer.c:349
    #6 0xa8eb710 in video_get_buffer ffmpeg/libavcodec/decode.c:1678:23
    #7 0xa8eb710 in avcodec_default_get_buffer2 ffmpeg/libavcodec/decode.c:1717
    #8 0xa90a8db in get_buffer_internal ffmpeg/libavcodec/decode.c:1945:11
    #9 0xa90a8db in ff_get_buffer ffmpeg/libavcodec/decode.c:1970

Thread T18 created by T0 here:
    #0 0x436f80 in pthread_create (ffmpeg_g+0x436f80)
    #1 0x2010fd0c in avpriv_slicethread_create ffmpeg/libavutil/slicethread.c:147:

Thread T1 created by T0 here:
    #0 0x436f80 in pthread_create (ffmpeg_g+0x436f80)
    #1 0x10ef97df in ff_frame_thread_init ffmpeg/libavcodec/pthread_frame.c:828:15
    #2 0x132987e8 in avcodec_open2 ffmpeg/libavcodec/utils.c:754:15
    #3 0x8795a6 in init_input_stream ffmpeg/fftools/ffmpeg.c:2939:20
    #4 0x8795a6 in transcode_init ffmpeg/fftools/ffmpeg.c:3696
    #5 0x82f7a0 in transcode ffmpeg/fftools/ffmpeg.c:4663:11
    #6 0x81cf5f in main ffmpeg/fftools/ffmpeg.c:4894:9
    #7 0x7fe17d350b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../c

SUMMARY: AddressSanitizer: heap-buffer-overflow ffmpeg/libavfilter/vf_yadif.c:138:
```

Please confirm.
Thanks

Attachments (2)

- gdb_vf_yadif_138(18.3 KB) - added by Suhwan 3 years ago.
- PoC_vf_yadif138.webp(336 bytes) - added by Suhwan 3 years ago.
  poc

Change History (5)

by Suhwan, 3 years ago

Attachment: *gdb_vf_yadif_138*added

by Suhwan, 3 years ago

Attachment: *PoC_vf_yadif138.webp*added

poc

comment:1 by Elon Musk, 23 months ago

Component: undetermined → avfilter
Reproduced by developer: set
Status: new → open

comment:2 by Michael Niedermayer, 19 months ago

Will post a patch fixing this

comment:3 by Michael Niedermayer, 19 months ago

Resolution: → fixed
Status: open → closed

Patch here: https://lists.ffmpeg.org/pipermail/ffmpeg-devel/2021-May/280739.html
will apply patch soon

Note: See TracTickets for help on using tickets.