#8310 closed defect (fixed)

Opened 3 years ago
Closed 3 years ago

heap-buffer-overflow at libavfilter/vf_lagfun.c:141

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/vf_lagfun.c:141 in lagfun_frame16
I compiled ffmpeg with "--toolchain=clang-asan" to check the memory corruption and attached log file.
How to reproduce:

```
% ffmpeg_g -stream_loop 25 -y -i $PoC -filter_complex lagfun -target vcd -loglevel

ffmpeg version N-95450-g1d479300cb 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

```
=================================================================
==22005==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7fc59e02101e a
WRITE of size 2 at 0x7fc59e02101e thread T60
    #0 0xe45857 in lagfun_frame16 ffmpeg/libavfilter/vf_lagfun.c:141:24
    #1 0x943139 in worker_func ffmpeg/libavfilter/pthread.c:50:15
    #2 0x86b8122 in run_jobs ffmpeg/libavutil/slicethread.c:61:9
    #3 0x86b5a8d in thread_worker ffmpeg/libavutil/slicethread.c:85:13
    #4 0x4eb9de in __asan::AsanThread::ThreadStart(unsigned long, __sanitizer::ato
    #5 0x7fc5cb2606da in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x76d
    #6 0x7fc5ca96588e in clone /build/glibc-OTsEL5/glibc-2.27/misc/../sysdeps/unix

0x7fc59e02101f is located 0 bytes to the right of 1280031-byte region [0x7fc59dee8
allocated by thread T0 here:
    #0 0x4de9e8 in posix_memalign (ffmpeg_g+0x4de9e8)
    #1 0x85c4251 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x852b181 in av_buffer_alloc ffmpeg/libavutil/buffer.c:72:12
    #3 0x852b181 in av_buffer_allocz ffmpeg/libavutil/buffer.c:85
    #4 0x852f9a6 in pool_alloc_buffer ffmpeg/libavutil/buffer.c:313:26
    #5 0x852f9a6 in av_buffer_pool_get ffmpeg/libavutil/buffer.c:349
    #6 0x91b6ed in ff_frame_pool_get ffmpeg/libavfilter/framepool.c:222:29
    #7 0x15d8e4c in ff_default_get_video_buffer ffmpeg/libavfilter/video.c:90:13
    #8 0xe3e4f5 in filter_frame ffmpeg/libavfilter/vf_lagfun.c:188:11
    #9 0x827129 in ff_filter_activate_default ffmpeg/libavfilter/avfilter.c:1084:1
    #10 0x827129 in ff_filter_activate ffmpeg/libavfilter/avfilter.c:1443
    #11 0x86ffd5 in push_frame ffmpeg/libavfilter/buffersrc.c:187:15
    #12 0x86ffd5 in av_buffersrc_add_frame_internal ffmpeg/libavfilter/buffersrc.c
    #13 0x86ea62 in av_buffersrc_add_frame_flags ffmpeg/libavfilter/buffersrc.c:17
    #14 0x666467 in ifilter_send_frame ffmpeg/fftools/ffmpeg.c:2186:11
    #15 0x666467 in send_frame_to_filters ffmpeg/fftools/ffmpeg.c:2260
    #16 0x6076c6 in decode_video ffmpeg/fftools/ffmpeg.c:2459:11
    #17 0x6076c6 in process_input_packet ffmpeg/fftools/ffmpeg.c:2613
    #18 0x641d1d in process_input ffmpeg/fftools/ffmpeg.c:4269:23
    #19 0x5e71b7 in transcode_step ffmpeg/fftools/ffmpeg.c:4628:11
    #20 0x5e71b7 in transcode ffmpeg/fftools/ffmpeg.c:4682
    #21 0x5db6bb in main ffmpeg/fftools/ffmpeg.c:4884:9
    #22 0x7fc5ca865b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../

Thread T60 created by T0 here:
    #0 0x436f80 in pthread_create (ffmpeg_g+0x436f80)
    #1 0x86b4c79 in avpriv_slicethread_create ffmpeg/libavutil/slicethread.c:147:1

SUMMARY: AddressSanitizer: heap-buffer-overflow ffmpeg/libavfilter/vf_lagfun.c:141
Shadow bytes around the buggy address:
  0x0ff933bfc1b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff933bfc1c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff933bfc1d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff933bfc1e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff933bfc1f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0ff933bfc200: 00 00 00[07]fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff933bfc210: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff933bfc220: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff933bfc230: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff933bfc240: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff933bfc250: 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
==22005==ABORTING
```

Please confirm.
Thanks

Attachments (1)

- PoC.exr(60.9 KB) - added by Suhwan 3 years ago.
  poc

Change History (2)

by Suhwan, 3 years ago

Attachment: *PoC.exr* added

poc

comment:1 by Elon Musk, 3 years ago

Resolution: → fixed
Status: new → closed

Note: See TracTickets for help on using tickets.