Opened 3 years ago
Closed 3 years ago

#8265 closed defect (fixed)

Division by zero at libavfilter/vf_lenscorrection.c:177

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

Description

Summary of the bug:
There is a Division by zero at libavfilter/vf_lenscorrection.c:177

How to reproduce:

```
% ffmpeg_g -y -i $PoC -filter_complex lenscorrection -loglevel 99 tmp.wtv

ffmpeg version N-95336-g4f4334bcbc 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 log

```
libavfilter/vf_lenscorrection.c:177:45: runtime error: division by zero
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior libavfilter/vf_lenscorrect

Thread 1 "ffmpeg_asan" received signal SIGFPE, Arithmetic exception.
0x0000000000e45a68 in filter_frame (inlink=<optimized out>, in=<optimized out>) at
177                 const int64_t r2inv = (4LL<<60) / (w * w + h * h);
(gdb) bt
#0  0x0000000000e45a68 in filter_frame (inlink=<optimized out>, in=<optimized out>
#1  0x0000000000826e2a in ff_filter_frame_framed (link=<optimized out>, frame=0x0)
#2  ff_filter_frame_to_filter (link=<optimized out>) at libavfilter/avfilter.c:121
#3  ff_filter_activate_default (filter=0x611000001080) at libavfilter/avfilter.c:1
#4  ff_filter_activate (filter=0x611000001080) at libavfilter/avfilter.c:1430
#5  0x000000000086fd23 in push_frame (graph=0x60e0000010c0) at libavfilter/buffers
#6  av_buffersrc_add_frame_internal (ctx=<optimized out>, frame=0x61600000e480, fl
#7  0x000000000086e763 in av_buffersrc_add_frame_flags (ctx=0x6110000011c0, frame=
#8  0x0000000000666408 in ifilter_send_frame (ifilter=<optimized out>, frame=<opti
#9  send_frame_to_filters (ist=0x615000000040, decoded_frame=0x61600000e480) at ff
#10 0x0000000000607667 in decode_video (ist=0x615000000040, pkt=0x7fff00000000, go
    at fftools/ffmpeg.c:2459
#11 process_input_packet (ist=0x615000000040, pkt=0x0, no_eof=0) at fftools/ffmpeg
#12 0x0000000000644c59 in process_input (file_index=0) at fftools/ffmpeg.c:4303
#13 0x00000000005e7158 in transcode_step () at fftools/ffmpeg.c:4628
#14 transcode () at fftools/ffmpeg.c:4682
#15 0x00000000005db65c in main (argc=<optimized out>, argv=<optimized out>) at fft
(gdb) disass $pc-32,$pc+32
Dump of assembler code from 0xe45a48 to 0xe45a88:
   0x0000000000e45a48 <filter_frame+4104>:      je     0xe4690a <filter_frame+7882
   0x0000000000e45a4e <filter_frame+4110>:      mov    $0xb340eac,%edi
   0x0000000000e45a53 <filter_frame+4115>:      callq  0x505ae0 <__sanitizer_cov_t
   0x0000000000e45a58 <filter_frame+4120>:      mov    0x68(%rbx),%r12
   0x0000000000e45a5c <filter_frame+4124>:      movabs $0x4000000000000000,%rax
   0x0000000000e45a66 <filter_frame+4134>:      cqto
=> 0x0000000000e45a68 <filter_frame+4136>:      idiv   %r14
   0x0000000000e45a6b <filter_frame+4139>:      mov    %rax,0x120(%rbx)
   0x0000000000e45a72 <filter_frame+4146>:      movslq 0x10(%rbx),%rdi
   0x0000000000e45a76 <filter_frame+4150>:      movslq 0x4(%rbx),%rsi
   0x0000000000e45a7a <filter_frame+4154>:      shl    $0x2,%rsi
   0x0000000000e45a7e <filter_frame+4158>:      callq  0x8598a50 <av_malloc_array>
   0x0000000000e45a83 <filter_frame+4163>:      mov    %rax,%r14
   0x0000000000e45a86 <filter_frame+4166>:      cmpb   $0x0,0x1(%rbx)
End of assembler dump.
(gdb) n
0x00000000004e2830 in __asan::AsanOnDeadlySignal(int, void*, void*) ()
(gdb) n
Single stepping until exit from function _ZN6__asan18AsanOnDeadlySignalEiPvS0_,
which has no line number information.
AddressSanitizer:DEADLYSIGNAL
=================================================================
==41795==ERROR: AddressSanitizer: FPE on unknown address 0x000000e45a68 (pc 0x0000
    #0 0xe45a67 in filter_frame ffmpeg/libavfilter/vf_lenscorrection.c:177:45
    #1 0x826e29 in ff_filter_activate_default ffmpeg/libavfilter/avfilter.c:1071:1
    #2 0x826e29 in ff_filter_activate ffmpeg/libavfilter/avfilter.c:1430
    #3 0x86fd22 in push_frame ffmpeg/libavfilter/buffersrc.c:187:15
    #4 0x86fd22 in av_buffersrc_add_frame_internal ffmpeg/libavfilter/buffersrc.c:
    #5 0x86e762 in av_buffersrc_add_frame_flags ffmpeg/libavfilter/buffersrc.c:170
    #6 0x666407 in ifilter_send_frame ffmpeg/fftools/ffmpeg.c:2186:11
    #7 0x666407 in send_frame_to_filters ffmpeg/fftools/ffmpeg.c:2260
    #8 0x607666 in decode_video ffmpeg/fftools/ffmpeg.c:2459:11
    #9 0x607666 in process_input_packet ffmpeg/fftools/ffmpeg.c:2613
    #10 0x644c58 in process_input ffmpeg/fftools/ffmpeg.c:4303:23
    #11 0x5e7157 in transcode_step ffmpeg/fftools/ffmpeg.c:4628:11
    #12 0x5e7157 in transcode ffmpeg/fftools/ffmpeg.c:4682
    #13 0x5db65b in main ffmpeg/fftools/ffmpeg.c:4884:9
    #14 0x7ffff5c93b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../
    #15 0x41def9 in _start (ffmpeg_asan+0x41def9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE ffmpeg/libavfilter/vf_lenscorrection.c:177:45 in fi
==41795==ABORTING
```

Please confirm.
Thanks

Attachments (2)

- gdb-vf_lenscorrection_177(14.8 KB) - added by Suhwan 3 years ago.
- PoC_vf_lenscorrection_177.png48(290 bytes) - added by Suhwan 3 years ago.
  poc

Change History (3)

by Suhwan, 3 years ago

Attachment: *gdb-vf_lenscorrection_177*added by Suhwan, 3 years ago

Attachment: *PoC_vf_lenscorrection_177.png48*added

poc

comment:1 by Elon Musk, 3 years ago

Resolution: → fixed
Status: new → closed

Note: See TracTickets for help on using tickets.