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

#8264 closed defect (fixed)

heap-buffer-overflow at libavfilter/vf_fieldorder.c

Reported by:	Suhwan	Owned by:	
Priority:	normal	Component:	avfilter
Version:	git-master	Keywords:	asan fieldorder
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_fieldorder.c in filter_frame
I compiled ffmpeg with "--toolchain=clang-asan" to check the memory corruption and attached log file.

How to reproduce:

```
% ffmpeg_g -y -i $PoC -filter_complex fieldorder -loglevel 99 tmp.h261

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 ASAN log

```
=================================================================
==15038==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61100000fec0 a
READ of size 4 at 0x61100000fec0 thread T0
    #0 0x4dcc71 in __asan_memcpy (ffmpeg_asan+0x4dcc71)
    #1 0xd57a9c in filter_frame ffmpeg/libavfilter/vf_fieldorder.c
    #2 0x826e29 in ff_filter_activate_default ffmpeg/libavfilter/avfilter.c:1071:1
    #3 0x826e29 in ff_filter_activate ffmpeg/libavfilter/avfilter.c:1430
    #4 0x86fcd5 in push_frame ffmpeg/libavfilter/buffersrc.c:187:15
    #5 0x86fcd5 in av_buffersrc_add_frame_internal ffmpeg/libavfilter/buffersrc.c:
    #6 0x86e762 in av_buffersrc_add_frame_flags ffmpeg/libavfilter/buffersrc.c:170
    #7 0x666407 in ifilter_send_frame ffmpeg/fftools/ffmpeg.c:2186:11
    #8 0x666407 in send_frame_to_filters ffmpeg/fftools/ffmpeg.c:2260
    #9 0x607666 in decode_video ffmpeg/fftools/ffmpeg.c:2459:11
    #10 0x607666 in process_input_packet ffmpeg/fftools/ffmpeg.c:2613
    #11 0x644c58 in process_input ffmpeg/fftools/ffmpeg.c:4303:23
    #12 0x5e7157 in transcode_step ffmpeg/fftools/ffmpeg.c:4628:11
    #13 0x5e7157 in transcode ffmpeg/fftools/ffmpeg.c:4682
    #14 0x5db65b in main ffmpeg/fftools/ffmpeg.c:4884:9
    #15 0x7ffff5c93b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../
    #16 0x41def9 in _start (ffmpeg_asan+0x41def9)

Address 0x61100000fec0 is a wild pointer.
SUMMARY: AddressSanitizer: heap-buffer-overflow (ffmpeg_asan+0x4dcc71) in __asan_m
```

Please confirm.
Thanks

Attachments (2)

- log_vf_fieldorder(12.3 KB) - added by Suhwan 3 years ago.
- PoC_vf_fieldorder.png32(311 bytes) - added by Suhwan 3 years ago.
  poc

Change History (4)

by Suhwan, 3 years ago

Attachment: *log_vf_fieldorder*added

by Suhwan, 3 years ago

Attachment: *PoC_vf_fieldorder.png32*added

poc

comment:1 by Elon Musk, 3 years ago

Resolution: → fixed
Status: new → closed

comment:2 by Carl Eugen Hoyos, 3 years ago

Component: undetermined → avfilter
Keywords: fieldorder added

Note: See TracTickets for help on using tickets.