#8246 closed defect (duplicate)

Opened 3 years ago
Closed 19 months ago

heap-buffer-overflow at libavfilter/vf_vmafmotion.c:179

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_vmafmotion.c:179 in convolution_y_8bit
I compiled ffmpeg with "--toolchain=clang-asan" to check the heap buffer overflow and attached log file.

How to reproduce:

```
% ffmpeg_g -t 1 -y -r 98 -i $PoC -filter_complex vmafmotion -target vcd -loglevel

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

```
==4009==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60a000000ca0 at
WRITE of size 2 at 0x60a000000ca0 thread T0
    #0 0x13c6186 in convolution_y_8bit ffmpeg/libavfilter/vf_vmafmotion.c:179:1
    #1 0x13bcaf8 in ff_vmafmotion_process ffmpeg/libavfilter/vf_vmafmotion.c:192:5
    #2 0x13c68f8 in do_vmafmotion ffmpeg/libavfilter/vf_vmafmotion.c:225:13
    #3 0x13c68f8 in filter_frame ffmpeg/libavfilter/vf_vmafmotion.c:300
    #4 0x827289 in ff_filter_activate_default ffmpeg/libavfilter/avfilter.c:1071:1
    #5 0x827289 in ff_filter_activate ffmpeg/libavfilter/avfilter.c:1430
    #6 0x870182 in push_frame ffmpeg/libavfilter/buffersrc.c:187:15
    #7 0x870182 in av_buffersrc_add_frame_internal ffmpeg/libavfilter/buffersrc.c:
    #8 0x86ebc2 in av_buffersrc_add_frame_flags ffmpeg/libavfilter/buffersrc.c:170
    #9 0x666867 in ifilter_send_frame ffmpeg/fftools/ffmpeg.c:2196:11
    #10 0x666867 in send_frame_to_filters ffmpeg/fftools/ffmpeg.c:2270
    #11 0x6075f7 in decode_video ffmpeg/fftools/ffmpeg.c:2469:11
    #12 0x6075f7 in process_input_packet ffmpeg/fftools/ffmpeg.c:2623
    #13 0x64ab67 in process_input ffmpeg/fftools/ffmpeg.c:4518:5
    #14 0x5e7157 in transcode_step ffmpeg/fftools/ffmpeg.c:4638:11
    #15 0x5e7157 in transcode ffmpeg/fftools/ffmpeg.c:4692
    #16 0x5db65b in main ffmpeg/fftools/ffmpeg.c:4894:9
    #17 0x7ffff5c93b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../
    #18 0x41def9 in _start (ffmpeg/ffmpeg_g+0x41def9)

0x60a000000ca0 is located 32 bytes to the left of 64-byte region [0x60a000000cc0,0
allocated by thread T0 here:
    #0 0x4de9e8 in posix_memalign (ffmpeg/ffmpeg_g+0x4de9e8)
    #1 0x8564fb1 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x13be241 in ff_vmafmotion_init ffmpeg/libavfilter/vf_vmafmotion.c:248:29

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

Please confirm.
Thanks

Attachments (2)

- gdb-vf_vmafmotion179(15.0 KB) - added by Suhwan 3 years ago.
- PoC_vf_vmafmotion_179.bmp(1.1 KB) - added by Suhwan 3 years ago.
  poc

Change History (3)

by Suhwan, 3 years ago

Attachment: *gdb-vf_vmafmotion179*added

by Suhwan, 3 years ago

Attachment: *PoC_vf_vmafmotion_179.bmp*added

poc

comment:1 by Michael Niedermayer, 19 months ago

Resolution: → duplicate
Status: new → closed

Duplicate of ~~#8241~~

Note: See TracTickets for help on using tickets.