#8241 closed defect (fixed)

Opened 3 years ago
Closed 19 months ago

heap-buffer-overflow at libavfilter/vf_vmafmotion.c

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:180 in convolution_y_10bit
I compiled ffmpeg with "--toolchain=clang-asan" to check the heap buffer overflow and attached log file.

How to reproduce:

```
% ffmpeg_g -stream_loop 1 -y -i samples/tmp3/tmp-33.png48 -filter_complex vmafmoti

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

```
=================================================================
==43591==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000007d60 a
READ of size 2 at 0x619000007d60 thread T0
    #0 0x13c447e in convolution_y_10bit ffmpeg/libavfilter/vf_vmafmotion.c:180:1
    #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 0x64211d in process_input ffmpeg/fftools/ffmpeg.c:4279:23
    #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)

0x619000007d60 is located 32 bytes to the left of 1055-byte region [0x619000007d80
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 0x84cc231 in av_buffer_alloc ffmpeg/libavutil/buffer.c:72:12
    #3 0x84cc231 in av_buffer_allocz ffmpeg/libavutil/buffer.c:85
    #4 0x84d0a56 in pool_alloc_buffer ffmpeg/libavutil/buffer.c:313:26
    #5 0x84d0a56 in av_buffer_pool_get ffmpeg/libavutil/buffer.c:349
    #6 0x91af8d in ff_frame_pool_get ffmpeg/libavfilter/framepool.c:222:29
    #7 0x15a660c in ff_default_get_video_buffer ffmpeg/libavfilter/video.c:90:13
    #8 0x124c7f9 in scale_frame ffmpeg/libavfilter/vf_scale.c:460:11
    #9 0x124a8ec in filter_frame ffmpeg/libavfilter/vf_scale.c:549:11
    #10 0x827289 in ff_filter_activate_default ffmpeg/libavfilter/avfilter.c:1071:
    #11 0x827289 in ff_filter_activate ffmpeg/libavfilter/avfilter.c:1430
    #12 0x870135 in push_frame ffmpeg/libavfilter/buffersrc.c:187:15
    #13 0x870135 in av_buffersrc_add_frame_internal ffmpeg/libavfilter/buffersrc.c
    #14 0x86ebc2 in av_buffersrc_add_frame_flags ffmpeg/libavfilter/buffersrc.c:17
    #15 0x666867 in ifilter_send_frame ffmpeg/fftools/ffmpeg.c:2196:11
    #16 0x666867 in send_frame_to_filters ffmpeg/fftools/ffmpeg.c:2270
    #17 0x6075f7 in decode_video ffmpeg/fftools/ffmpeg.c:2469:11
    #18 0x6075f7 in process_input_packet ffmpeg/fftools/ffmpeg.c:2623
    #19 0x64211d in process_input ffmpeg/fftools/ffmpeg.c:4279:23
    #20 0x5e7157 in transcode_step ffmpeg/fftools/ffmpeg.c:4638:11
    #21 0x5e7157 in transcode ffmpeg/fftools/ffmpeg.c:4692
    #22 0x5db65b in main ffmpeg/fftools/ffmpeg.c:4894:9
    #23 0x7ffff5c93b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../

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

Please confirm.
Thanks

Attachments (2)

- gdb_vf_vmafmotion180(17.1 KB) - added by Suhwan 3 years ago.
- PoC_vf_vmafmotion180.png48(290 bytes) - added by Suhwan 3 years ago.
  poc

Change History (5)

comment:1 by Suhwan, 3 years ago

How to reproduce:

```
% ffmpeg_g -stream_loop 1 -y -i $PoC -filter_complex vmafmotion -target dvd -loglev

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=clang-
```

by Suhwan, 3 years ago

Attachment: *gdb_vf_vmafmotion180*added

by Suhwan, 3 years ago

Attachment: *PoC_vf_vmafmotion180.png48*added

poc

comment:2 by Michael Niedermayer, 19 months ago

Will submit a patch to ffmpeg-devel

comment:3 by Michael Niedermayer, 19 months ago

Resolution: → fixed
Status: new → closed

Patch here: https://lists.ffmpeg.org/pipermail/ffmpeg-devel/2021-May/280737.html
will apply patch soon

Note: See TracTickets for help on using tickets.