

heap-buffer-overflow at libavfilter/vf_neighbor.c

Reported by:	Suhwan	Owned by:	
Priority:	normal	Component:	avfilter
Version:	git-master	Keywords:	neighbor 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_neighbor.c:191 in deflate16
I compiled ffmpeg with "--toolchain=clang-asan" to check the heap buffer overflow and attached log file.
How to reproduce:

```
% ffmpeg -y -i samples/tmp3/tmp-32.png48 -filter_complex deflate -target dvd -lo
ffmpeg version N-95314-g1331e00179 Copyright (c) 2000-2019 the FFmpeg developers
built with clang version 6.0.0-lubuntu2 (tags/RELEASE_600/final)
configuration: --cc=clang --cxx=clang++ --ld=clang --enable-debug --toolchain=clang
```

Here's ASAN log

```
==41359==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000007d7e a
READ of size 2 at 0x619000007d7e thread T0
#0 0x103878f in deflate16 ffmpeg/libavfilter/vf_neighbor.c:191:35
#1 0x1033f4b in filter_slice ffmpeg/libavfilter/vf_neighbor.c:301:13
#2 0x9429d9 in worker_func ffmpeg/libavfilter/pthread.c:50:15
#3 0x8658de2 in run_jobs ffmpeg/libavutil/slicethread.c:61:9
#4 0x8658484 in avpriv_slicethread_execute ffmpeg/libavutil/slicethread.c:188:
#5 0x942136 in thread_execute ffmpeg/libavfilter/pthread.c:72:5
#6 0x102f611 in filter_frame ffmpeg/libavfilter/vf_neighbor.c:328:5
#7 0x827289 in ff_filter_activate_default ffmpeg/libavfilter/avfilter.c:1071:1
#8 0x827289 in ff_filter_activate ffmpeg/libavfilter/avfilter.c:1430
#9 0x870182 in push_frame ffmpeg/libavfilter/buffersrc.c:187:15
#10 0x870182 in av_buffersrc_add_frame_internal ffmpeg/libavfilter/buffersrc.c:1
#11 0x86ebc2 in av_buffersrc_add_frame_flags ffmpeg/libavfilter/buffersrc.c:17
#12 0x66867 in ifilter_send_frame ffmpeg/fftools/ffmpeg.c:2196:11
#13 0x66867 in send_frame_to_filters ffmpeg/fftools/ffmpeg.c:2270
#14 0x6075f7 in decode_video ffmpeg/fftools/ffmpeg.c:2469:11
#15 0x6075f7 in process_input_packet ffmpeg/fftools/ffmpeg.c:2623
#16 0x6450b8 in process_input ffmpeg/fftools/ffmpeg.c:4313:23
#17 0x5e7157 in transcode_step ffmpeg/fftools/ffmpeg.c:4638:11
#18 0x5e7157 in transcode ffmpeg/fftools/ffmpeg.c:4692
#19 0x5db65b in main ffmpeg/fftools/ffmpeg.c:4894:9
#20 0x7ffff5c93b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/./
#21 0x41def9 in _start (ffmpeg/ffmpeg_g+0x41def9)

0x619000007d7e is located 2 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 0x66867 in ifilter_send_frame ffmpeg/fftools/ffmpeg.c:2196:11
#16 0x66867 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 0x6450b8 in process_input ffmpeg/fftools/ffmpeg.c:4313:23
#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_neighbor.c:1
```

Please confirm.
Thanks

Attachments (2)

- [gdb-vf_neighbor_191](#) (17.0 KB) - added by Suhwan 3 years ago.
- [PoC_vf_neighbor_191.png48](#) (290 bytes) - added by Suhwan 3 years ago.

Change History (4)

by Suhwan, 3 years ago	Attachment: gdb-vf_neighbor_191 added
by Suhwan, 3 years ago	Attachment: PoC_vf_neighbor_191.png48 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: neighbor added

[e787f8fd7ee99ba0c3e0f086ce2ce59eea7ed86c](#)

Note: See [TracTickets](#) for help on using tickets.