

heap-buffer-overflow at libavfilter/vf_bwdif.c:133

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_bwdif.c:133 in filter_intra

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 bwdif -target dvd -loglevel 99 tmp.h263

ffmpeg version N-95336-g4f4334bcbc 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

```
=====
==15693==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000002d60 a
READ of size 1 at 0x619000002d60 thread T0
#0 0xa7954f in filter_intra ffmpeg/libavfilter/vf_bwdif.c:133:5
#1 0xa816b4 in filter_slice ffmpeg/libavfilter/vf_bwdif.c:236:17
#2 0x942579 in worker_func ffmpeg/libavfilter/pthread.c:50:15
#3 0x868c042 in run_jobs ffmpeg/libavutil/slicethread.c:61:9
#4 0x868b6e4 in avpriv_slicethread_execute ffmpeg/libavutil/slicethread.c:188:
#5 0x941cd6 in thread_execute ffmpeg/libavfilter/pthread.c:72:5
#6 0xa73691 in filter_ffmpeg/libavfilter/vf_bwdif.c:283:9
#7 0x163bd0c in return_frame ffmpeg/libavfilter/yadif_common.c:51:5
#8 0x163ddf9 in ff_yadif_request_frame ffmpeg/libavfilter/yadif_common.c:166:9
#9 0x831204 in ff_request_frame_to_filter ffmpeg/libavfilter/avfilter.c:458:15
#10 0x826f74 in ff_filter_activate ffmpeg/libavfilter/avfilter.c:1280:20
#11 0x864092 in get_frame_internal ffmpeg/libavfilter/buffersink.c:110:19
#12 0x84bd53 in avfilter_graph_request_oldest ffmpeg/libavfilter/avfiltergraph
#13 0x5e3d0d in transcode_from_filter ffmpeg/fftools/ffmpeg.c:4531:11
#14 0x5e3d0d in transcode_step ffmpeg/fftools/ffmpeg.c:4606
#15 0x5e3d0d in transcode ffmpeg/fftools/ffmpeg.c:4682
#16 0x5db65b in main ffmpeg/fftools/ffmpeg.c:4884:9
#17 0x7fff5c93b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/./
#18 0x41def9 in _start (ffmpeg_asan+0x41def9)

0x619000002d60 is located 32 bytes to the left of 1055-byte region [0x619000002d80
allocated by thread T0 here:
#0 0x4de9e8 in posix_memalign (ffmpeg_asan+0x4de9e8)
#1 0x8598211 in av_malloc ffmpeg/libavutil/mem.c:87:9
#2 0x84ff141 in av_buffer_alloc ffmpeg/libavutil/buffer.c:72:12
#3 0x84ff141 in av_buffer_allocz ffmpeg/libavutil/buffer.c:85
#4 0x8503966 in pool_alloc_buffer ffmpeg/libavutil/buffer.c:313:26
#5 0x8503966 in av_buffer_pool_get ffmpeg/libavutil/buffer.c:349
#6 0x91ab2d in ff_frame_pool_get ffmpeg/libavfilter/framepool.c:222:29
#7 0x15d770c in ff_default_get_video_buffer ffmpeg/libavfilter/video.c:90:13
#8 0x124c5c9 in scale_frame ffmpeg/libavfilter/vf_scale.c:460:11
#9 0x124a6bc in filter_frame ffmpeg/libavfilter/vf_scale.c:549:11
#10 0x826e29 in ff_filter_activate_default ffmpeg/libavfilter/avfilter.c:1071:
#11 0x826e29 in ff_filter_activate ffmpeg/libavfilter/avfilter.c:1430
#12 0x86fcd5 in push_frame ffmpeg/libavfilter/buffersrc.c:187:15
#13 0x86fcd5 in av_buffersrc_add_frame_internal ffmpeg/libavfilter/buffersrc.c
#14 0x86e762 in av_buffersrc_add_frame_flags ffmpeg/libavfilter/buffersrc.c:17
#15 0x666407 in ifilter_send_frame ffmpeg/fftools/ffmpeg.c:2186:11
#16 0x666407 in send_frame_to_filters ffmpeg/fftools/ffmpeg.c:2260
#17 0x607666 in decode_video ffmpeg/fftools/ffmpeg.c:2459:11
#18 0x607666 in process_input_packet ffmpeg/fftools/ffmpeg.c:2613
#19 0x64a707 in process_input ffmpeg/fftools/ffmpeg.c:4508:5
#20 0x5e7157 in transcode_step ffmpeg/fftools/ffmpeg.c:4628:11
#21 0x5e7157 in transcode ffmpeg/fftools/ffmpeg.c:4682
#22 0x5db65b in main ffmpeg/fftools/ffmpeg.c:4884:9
#23 0x7fff5c93b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/./

SUMMARY: AddressSanitizer: heap-buffer-overflow ffmpeg/libavfilter/vf_bwdif.c:133:
```

Please confirm.
Thanks

Attachments (2)

- log_vf_bwdif_133(15.8 KB) - added by Suhwan 3 years ago.
- PoC_vf_bwdif_133.bmp(90 bytes) - added by Suhwan 3 years ago.
poc

Change History (3)

by Suhwan, 3 years ago
Attachment: log_vf_bwdif_133 added
by Suhwan, 3 years ago
Attachment: PoC_vf_bwdif_133.bmp added
poc
comment:1 by Elon Musk, 3 years ago
Resolution: → fixed
Status: new → closed

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