#8296 closed defect (fixed)

Opened 3 years ago
Closed 3 years ago

memory leaks from av_buffersrc_add_frame_flags()

Reported by:	Suhwan	Owned by:	
Priority:	important	Component:	undetermined
Version:	git-master	Keywords:	
Cc:		Blocked By:	
Blocking:		Reproduced by developer:	no
Analyzed by developer:	no		

Description

Summary of the bug:
There are memory leaks from av_buffersrc_add_frame_flags()
How to reproduce:

```
% ffmpeg_g -y -i $PoC -filter_complex random -target dv50 -loglevel 0 -vbsf mjpeg2

ffmpeg version N-95425-g1e35519fe0 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
```

Here's Valgrind log

```
==34566== HEAP SUMMARY:
==34566==     in use at exit: 16,558 bytes in 20 blocks
==34566==   total heap usage: 3,798 allocs, 3,778 frees, 4,820,806 bytes allocated
==34566==
==34566== 16,526 (536 direct, 15,990 indirect) bytes in 1 blocks are definitely lo
==34566==    at 0x9FDFE76: memalign (in /usr/lib/valgrind/vgpreload_memcheck-amd64
==34566==    by 0x9FDFF91: posix_memalign (in /usr/lib/valgrind/vgpreload_memcheck
==34566==    by 0x592C189: av_malloc (mem.c:87)
==34566==    by 0x592C189: av_mallocz (mem.c:238)
==34566==    by 0x590031D: av_frame_alloc (frame.c:191)
==34566==    by 0x5F4170: av_buffersrc_add_frame_internal (buffersrc.c:237)
==34566==    by 0x5F2E7D: av_buffersrc_add_frame_flags (buffersrc.c:170)
==34566==    by 0x4CAD5F: ifilter_send_frame (ffmpeg.c:2186)
==34566==    by 0x4CAD5F: send_frame_to_filters (ffmpeg.c:2260)
==34566==    by 0x4A07BB: decode_video (ffmpeg.c:2459)
==34566==    by 0x4A07BB: process_input_packet (ffmpeg.c:2613)
==34566==    by 0x4BA037: process_input (ffmpeg.c:4303)
==34566==    by 0x48D5EA: transcode_step (ffmpeg.c:4628)
==34566==    by 0x48D5EA: transcode (ffmpeg.c:4682)
==34566==    by 0x487DA3: main (ffmpeg.c:4884)
==34566==
==34566== LEAK SUMMARY:
==34566==    definitely lost: 536 bytes in 1 blocks
==34566==    indirectly lost: 15,990 bytes in 18 blocks
==34566==      possibly lost: 0 bytes in 0 blocks
==34566==    still reachable: 32 bytes in 1 blocks
==34566==         suppressed: 0 bytes in 0 blocks
==34566== Reachable blocks (those to which a pointer was found) are not shown.
==34566== To see them, rerun with: --leak-check=full --show-leak-kinds=all
==34566==
==34566== For counts of detected and suppressed errors, rerun with: -v
==34566== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
```

ASAN log.

```
=================================================================
==17259==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 536 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_usan+0x4de9e8)
    #1 0x85c2178 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x85c2178 in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x856c977 in av_frame_alloc ffmpeg/libavutil/frame.c:191:22
    #4 0x86eaf2 in av_buffersrc_add_frame_flags ffmpeg/libavfilter/buffersrc.c:170
    #5 0x666407 in ifilter_send_frame ffmpeg/fftools/ffmpeg.c:2186:11
    #6 0x666407 in send_frame_to_filters ffmpeg/fftools/ffmpeg.c:2260
    #7 0x607666 in decode_video ffmpeg/fftools/ffmpeg.c:2459:11
    #8 0x607666 in process_input_packet ffmpeg/fftools/ffmpeg.c:2613
    #9 0x644c58 in process_input ffmpeg/fftools/ffmpeg.c:4303:23
    #10 0x5e7157 in transcode_step ffmpeg/fftools/ffmpeg.c:4628:11
    #11 0x5e7157 in transcode ffmpeg/fftools/ffmpeg.c:4682
    #12 0x5db65b in main ffmpeg/fftools/ffmpeg.c:4884:9
    #13 0x7f7cbca03b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../

Indirect leak of 15439 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_usan+0x4de9e8)
    #1 0x85c1021 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x8527f51 in av_buffer_alloc ffmpeg/libavutil/buffer.c:72:12
    #3 0x8527f51 in av_buffer_allocz ffmpeg/libavutil/buffer.c:85
    #4 0x852c776 in pool_alloc_buffer ffmpeg/libavutil/buffer.c:313:26
    #5 0x852c776 in av_buffer_pool_get ffmpeg/libavutil/buffer.c:349
    #6 0x2ef03a2 in video_get_buffer ffmpeg/libavcodec/decode.c:1678:23
    #7 0x2ef03a2 in avcodec_default_get_buffer2 ffmpeg/libavcodec/decode.c:1717
    #8 0x2ef7eac in get_buffer_internal ffmpeg/libavcodec/decode.c:1945:11
    #9 0x2ef7eac in ff_get_buffer ffmpeg/libavcodec/decode.c:1970

Indirect leak of 95 byte(s) in 6 object(s) allocated from:
    #0 0x4de230 in realloc (ffmpeg_usan+0x4de230)
    #1 0x85c2be7 in av_realloc ffmpeg/libavutil/mem.c:144:12
    #2 0x85c2be7 in av_strdup ffmpeg/libavutil/mem.c:256
    #3 0x853981d in av_dict_copy ffmpeg/libavutil/dict.c:222:19

Indirect leak of 88 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_usan+0x4de9e8)
    #1 0x85c1021 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x8527dcd in av_buffer_alloc ffmpeg/libavutil/buffer.c:72:12
    #3 0x856b423 in av_frame_new_side_data ffmpeg/libavutil/frame.c:727:24
    #4 0x85b9419 in av_mastering_display_metadata_create_side_data ffmpeg/libavuti
    #5 0x47532c3 in decode_frame_png ffmpeg/libavcodec/pngdec.c:1474:16
    #6 0x48495d6 in frame_worker_thread ffmpeg/libavcodec/pthread_frame.c:201:21

Indirect leak of 88 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_usan+0x4de9e8)
    #1 0x85c2178 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x85c2178 in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x852b093 in av_buffer_pool_init ffmpeg/libavutil/buffer.c:240:26

Indirect leak of 48 byte(s) in 1 object(s) allocated from:
    #0 0x4de230 in realloc (ffmpeg_usan+0x4de230)
    #1 0x8537020 in av_dict_set ffmpeg/libavutil/dict.c:106:34
    #2 0x853981d in av_dict_copy ffmpeg/libavutil/dict.c:222:19
```

```
Indirect leak of 40 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_usan+0x4de9e8)
    #1 0x85c2178 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x85c2178 in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x852c7a6 in pool_alloc_buffer ffmpeg/libavutil/buffer.c:317:11
    #4 0x852c7a6 in av_buffer_pool_get ffmpeg/libavutil/buffer.c:349
    #5 0x2ef03a2 in video_get_buffer ffmpeg/libavcodec/decode.c:1678:23
    #6 0x2ef03a2 in avcodec_default_get_buffer2 ffmpeg/libavcodec/decode.c:1717
    #7 0x2ef7eac in get_buffer_internal ffmpeg/libavcodec/decode.c:1945:11
    #8 0x2ef7eac in ff_get_buffer ffmpeg/libavcodec/decode.c:1970

Indirect leak of 40 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_usan+0x4de9e8)
    #1 0x85c2178 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x85c2178 in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x8527438 in av_buffer_create ffmpeg/libavutil/buffer.c:35:11
    #4 0x8527f86 in av_buffer_alloc ffmpeg/libavutil/buffer.c:76:11
    #5 0x8527f86 in av_buffer_allocz ffmpeg/libavutil/buffer.c:85
    #6 0x852c776 in pool_alloc_buffer ffmpeg/libavutil/buffer.c:313:26
    #7 0x852c776 in av_buffer_pool_get ffmpeg/libavutil/buffer.c:349
    #8 0x2ef03a2 in video_get_buffer ffmpeg/libavcodec/decode.c:1678:23
    #9 0x2ef03a2 in avcodec_default_get_buffer2 ffmpeg/libavcodec/decode.c:1717
    #10 0x2ef7eac in get_buffer_internal ffmpeg/libavcodec/decode.c:1945:11
    #11 0x2ef7eac in ff_get_buffer ffmpeg/libavcodec/decode.c:1970

Indirect leak of 40 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_usan+0x4de9e8)
    #1 0x85c2178 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x85c2178 in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x856aa29 in av_frame_new_side_data_from_buf ffmpeg/libavutil/frame.c:708:1

Indirect leak of 40 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_usan+0x4de9e8)
    #1 0x85c2178 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x85c2178 in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x8527438 in av_buffer_create ffmpeg/libavutil/buffer.c:35:11
    #4 0x8527dff in av_buffer_alloc ffmpeg/libavutil/buffer.c:76:11
    #5 0x856b423 in av_frame_new_side_data ffmpeg/libavutil/frame.c:727:24
    #6 0x85b9419 in av_mastering_display_metadata_create_side_data ffmpeg/libavuti
    #7 0x47532c3 in decode_frame_png ffmpeg/libavcodec/pngdec.c:1474:16
    #8 0x48495d6 in frame_worker_thread ffmpeg/libavcodec/pthread_frame.c:201:21

Indirect leak of 24 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_usan+0x4de9e8)
    #1 0x85c2178 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x85c2178 in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x852816b in av_buffer_ref ffmpeg/libavutil/buffer.c:95:24

Indirect leak of 24 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_usan+0x4de9e8)
    #1 0x85c2178 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x85c2178 in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x852816b in av_buffer_ref ffmpeg/libavutil/buffer.c:95:24
    #4 0x8573eee in av_frame_ref ffmpeg/libavutil/frame.c:457:11

Indirect leak of 16 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_usan+0x4de9e8)
    #1 0x85c2178 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x85c2178 in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x8536e6e in av_dict_set ffmpeg/libavutil/dict.c:89:19
    #4 0x853981d in av_dict_copy ffmpeg/libavutil/dict.c:222:19

Indirect leak of 8 byte(s) in 1 object(s) allocated from:
    #0 0x4de230 in realloc (ffmpeg_usan+0x4de230)
    #1 0x856a9d0 in av_frame_new_side_data_from_buf ffmpeg/libavutil/frame.c:702:1

SUMMARY: AddressSanitizer: 16526 byte(s) leaked in 19 allocation(s).
```

Please confirm.
Thanks

Attachments (1)

- PoC_av_buf.png24(6.9 KB) - added by Suhwan 3 years ago.
  poc

Change History (2)

by Suhwan, 3 years ago

Attachment: *PoC_av_buf.png24*added

poc

comment:1 by Elon Musk, 3 years ago

Resolution: → fixed
Status: new → closed

Note: See TracTickets for help on using tickets.