#8285 closed defect (fixed)

Opened 3 years ago
Closed 2 years ago
Last modified 2 years ago

memory leaks in ff_v4l2_m2m_create_context()

Reported by:	Suhwan	Owned by:	
Priority:	normal	Component:	avcodec
Version:	git-master	Keywords:	v4l2m2m leak
Cc:		Blocked By:	
Blocking:		Reproduced by developer:	no
Analyzed by developer:	no		

Description

Summary of the bug:
There are memory leaks in ff_v4l2_m2m_create_context()
How to reproduce:

```
% ffmpeg_g -y -i $PoC -loglevel 0 tmp.m4v

ffmpeg version N-95389-gdd01947397 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

```
==10320== HEAP SUMMARY:
==10320==     in use at exit: 4,904 bytes in 4 blocks
==10320==   total heap usage: 5,333 allocs, 5,329 frees, 4,747,615 bytes allocated
==10320==
==10320== 4,872 (4,808 direct, 64 indirect) bytes in 1 blocks are definitely lost
==10320==    at 0x9D3CE76: memalign (in /usr/lib/valgrind/vgpreload_memcheck-amd64
==10320==    by 0x9D3CF91: posix_memalign (in /usr/lib/valgrind/vgpreload_memcheck
==10320==    by 0x590EC79: av_malloc (mem.c:87)
==10320==    by 0x590EC79: av_mallocz (mem.c:238)
==10320==    by 0x511ECEB: ff_v4l2_m2m_create_context (v4l2_m2m.c:399)
==10320==    by 0x3498507: v4l2_encode_init (v4l2_m2m_enc.c:293)
==10320==    by 0x3450C24: avcodec_open2 (utils.c:946)
==10320==    by 0x4A67F1: init_output_stream (ffmpeg.c:3507)
==10320==    by 0x4BFF95: reap_filters (ffmpeg.c:1442)
==10320==    by 0x48D611: transcode_step (ffmpeg.c:4638)
==10320==    by 0x48D611: transcode (ffmpeg.c:4682)
==10320==    by 0x487D53: main (ffmpeg.c:4884)
==10320==
==10320== LEAK SUMMARY:
==10320==    definitely lost: 4,808 bytes in 1 blocks
==10320==    indirectly lost: 64 bytes in 2 blocks
==10320==      possibly lost: 0 bytes in 0 blocks
==10320==    still reachable: 32 bytes in 1 blocks
==10320==         suppressed: 0 bytes in 0 blocks
==10320== Reachable blocks (those to which a pointer was found) are not shown.
==10320== To see them, rerun with: --leak-check=full --show-leak-kinds=all
==10320==
==10320== For counts of detected and suppressed errors, rerun with: -v
==10320== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
```

ASAN log.

```
=================================================================
==4711==ERROR: LeakSanitizer: detected memory leaks

Indirect leak of 4808 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_asan+0x4de9e8)
    #1 0x8594168 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x8594168 in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x7a66f79 in ff_v4l2_m2m_create_context ffmpeg/libavcodec/v4l2_m2m.c:399:10
    #4 0x50f50bc in avcodec_open2 ffmpeg/libavcodec/utils.c:946:15
    #5 0x61c29b in init_output_stream ffmpeg/fftools/ffmpeg.c:3507:20
    #6 0x654dea in reap_filters ffmpeg/fftools/ffmpeg.c:1442:19
    #7 0x5e73a2 in transcode_step ffmpeg/fftools/ffmpeg.c:4638:12
    #8 0x5e73a2 in transcode ffmpeg/fftools/ffmpeg.c:4682
    #9 0x5db65b in main ffmpeg/fftools/ffmpeg.c:4884:9
    #10 0x7f9d6580eb96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../

Indirect leak of 40 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_asan+0x4de9e8)
    #1 0x8594168 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x8594168 in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x84f9428 in av_buffer_create ffmpeg/libavutil/buffer.c:35:11
    #4 0x7a6701a in ff_v4l2_m2m_create_context ffmpeg/libavcodec/v4l2_m2m.c:403:25

Indirect leak of 24 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_asan+0x4de9e8)
    #1 0x8594168 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x8594168 in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x84f983e in av_buffer_create ffmpeg/libavutil/buffer.c:49:11
    #4 0x7a6701a in ff_v4l2_m2m_create_context ffmpeg/libavcodec/v4l2_m2m.c:403:25

SUMMARY: AddressSanitizer: 4872 byte(s) leaked in 3 allocation(s).
```

Please confirm.
Thanks

Attachments (1)

- PoC_ff_v4l2.mpeg(830.0 KB) - added by Suhwan 3 years ago.
  poc

Change History (5)

by Suhwan, 3 years ago

Attachment: *PoC_ff_v4l2.mpeg*added

poc

comment:1 by Carl Eugen Hoyos, 3 years ago

Component: undetermined → avcodec

Keywords: v4l2m2m leak added
Priority: important → normal

comment:2 by Balling, 2 years ago

Status: new → open

https://patchwork.ffmpeg.org/project/ffmpeg/patch/20200719193618.60977-1-andriy.gelman@gmail.com/

comment:3 by Andriy Gelman, 2 years ago

Fixed in 7c32e9cf93b712f8463573a59ed4e98fd10fa013

Last edited 2 years ago by Carl Eugen Hoyos (previous) (diff)

comment:4 by Andriy Gelman, 2 years ago

Resolution: → fixed
Status: open → closed

Note: See TracTickets for help on using tickets.