#8281 closed defect (fixed)

memory leaks from options.c:158 in avcodec_alloc_context3

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

Description

Summary of the bug:
There are memory leaks maybe from options.c:158 in avcodec_alloc_context3

How to reproduce:

```
% ffmpeg_g -y -i $PoC -loglevel 0 -vbsf h264_mp4toannexb -c:a:139 msmpeg4 -disposi

ffmpeg version N-95385-ge1b89c76f6 Copyright (c) 2000-2019 the FFmpeg developers
built with clang version 6.0.0-1ubuntu2 (tags/RELEASE_600/final)
```

Valgrind log.

```
==46857==
==46857==
==46857== HEAP SUMMARY:
==46857==     in use at exit: 1,096 bytes in 2 blocks
==46857==   total heap usage: 2,770 allocs, 2,768 frees, 3,927,957 bytes allocated
==46857==
==46857== 1,064 bytes in 1 blocks are definitely lost in loss record 2 of 2
==46857==    at 0x9D3BE76: memalign (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
==46857==    by 0x9D3BF91: posix_memalign (in /usr/lib/valgrind/vgpreload_memcheck-
==46857==    by 0x590E23D: av_malloc (mem.c:87)
==46857==    by 0x2D4E740: avcodec_alloc_context3 (options.c:158)
==46857==    by 0x2153CFC: ff_frame_thread_encoder_init (frame_thread_encoder.c:19
==46857==    by 0x344D15F: avcodec_open2 (utils.c:740)
==46857==    by 0x4A67F1: init_output_stream (ffmpeg.c:3507)
==46857==    by 0x4BFF95: reap_filters (ffmpeg.c:1442)
==46857==    by 0x48D611: transcode_step (ffmpeg.c:4638)
==46857==    by 0x48D611: transcode (ffmpeg.c:4682)
==46857==    by 0x487D53: main (ffmpeg.c:4884)
==46857==
==46857== LEAK SUMMARY:
==46857==    definitely lost: 1,064 bytes in 1 blocks
==46857==    indirectly lost: 0 bytes in 0 blocks
==46857==      possibly lost: 0 bytes in 0 blocks
==46857==    still reachable: 32 bytes in 1 blocks
==46857==         suppressed: 0 bytes in 0 blocks
==46857== Reachable blocks (those to which a pointer was found) are not shown.
==46857== To see them, rerun with: --leak-check=full --show-leak-kinds=all
==46857==
==46857== For counts of detected and suppressed errors, rerun with: -v
==46857== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
```

Attachments (1)

- PoC_option158.jpg(112.3 KB) - added by Suhwan 3 years ago.
  poc

Change History (3)

---

by Suhwan, 3 years ago

Attachment: *PoC_option158.jpg*added

poc

---

comment:1 by Carl Eugen Hoyos, 3 years ago

Component:	undetermined → avcodec
Keywords:	leak added
Priority:	normal → minor
Reproduced by developer:	set
Status:	new → open

comment:2 by mkver, 16 months ago

Resolution:	→ fixed
Status:	open → closed

Fixed in 7bba0dd6382e30d646cb406034a66199e071d713.

Note: See TracTickets for help on using tickets.