#8294 closed defect (fixed)

Opened 3 years ago
Closed 3 years ago

memory leaks in avpriv_float_dsp_alloc()

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 in avpriv_float_dsp_alloc()
How to reproduce:

```
% ffmpeg_g -y  -i $PoC -loglevel 0 -psnr tmp.eac3

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

```
==16402== HEAP SUMMARY:
==16402==     in use at exit: 120 bytes in 2 blocks
==16402==   total heap usage: 889 allocs, 887 frees, 2,885,023 bytes allocated
==16402==
==16402== 88 bytes in 1 blocks are definitely lost in loss record 2 of 2
==16402==    at 0x9FDFE76: memalign (in /usr/lib/valgrind/vgpreload_memcheck-amd64
==16402==    by 0x9FDFF91: posix_memalign (in /usr/lib/valgrind/vgpreload_memcheck
==16402==    by 0x592C189: av_malloc (mem.c:87)
==16402==    by 0x592C189: av_mallocz (mem.c:238)
==16402==    by 0x58FC61E: avpriv_float_dsp_alloc (float_dsp.c:137)
==16402==    by 0x44EB76E: ff_ac3_float_encode_init (ac3enc_float.c:135)
==16402==    by 0x346DC34: avcodec_open2 (utils.c:946)
==16402==    by 0x4A6841: init_output_stream (ffmpeg.c:3507)
==16402==    by 0x4BFFE5: reap_filters (ffmpeg.c:1442)
==16402==    by 0x48D661: transcode_step (ffmpeg.c:4638)
==16402==    by 0x48D661: transcode (ffmpeg.c:4682)
==16402==    by 0x487DA3: main (ffmpeg.c:4884)
==16402==
==16402== LEAK SUMMARY:
==16402==    definitely lost: 88 bytes in 1 blocks
==16402==    indirectly lost: 0 bytes in 0 blocks
==16402==      possibly lost: 0 bytes in 0 blocks
==16402==    still reachable: 32 bytes in 1 blocks
==16402==         suppressed: 0 bytes in 0 blocks
==16402== Reachable blocks (those to which a pointer was found) are not shown.
==16402== To see them, rerun with: --leak-check=full --show-leak-kinds=all
==16402==
==16402== For counts of detected and suppressed errors, rerun with: -v
==16402== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
```

ASAN log.

```
=================================================================
==33197==ERROR: LeakSanitizer: detected memory leaks

Direct 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 0x85651c0 in avpriv_float_dsp_alloc ffmpeg/libavutil/float_dsp.c:137:31

SUMMARY: AddressSanitizer: 88 byte(s) leaked in 1 allocation(s).
```

Please confirm.
Thanks

Attachments (1)

- PoC_avpriv.wav(125.0 KB) - added by Suhwan 3 years ago.
  poc

Change History (2)

by Suhwan, 3 years ago

Attachment: *PoC_avpriv.wav*added

poc

comment:1 by Elon Musk, 3 years ago

Resolution: → fixed
Status: new → closed

Note: See TracTickets for help on using tickets.