#8267 closed defect (fixed)

Opened 3 years ago
Closed 2 years ago

memory leaks from libavfilter/graphparser.c in link_filter_inouts

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

Description

Summary of the bug:
There're memory leaks from libavfilter/graphparser.c in link_filter_inouts

How to reproduce:

```
% ffmpeg_g -y -i $PoC -filter_complex rgbtestsrc -loglevel 0 tmp.mpegtsraw

ffmpeg version N-95336-g4f4334bcbc 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

```
==30745== HEAP SUMMARY:
==30745==     in use at exit: 612 bytes in 16 blocks
==30745==   total heap usage: 389 allocs, 373 frees, 2,471,014 bytes allocated
==30745==
==30745== 32 bytes in 1 blocks are definitely lost in loss record 11 of 15
==30745==    at 0x9D40E76: memalign (in /usr/lib/valgrind/vgpreload_memcheck-amd64
==30745==    by 0x9D40F91: posix_memalign (in /usr/lib/valgrind/vgpreload_memcheck
==30745==    by 0x5911E09: av_malloc (mem.c:87)
==30745==    by 0x5911E09: av_mallocz (mem.c:238)
==30745==    by 0x65F62E: link_filter_inouts (graphparser.c:285)
==30745==    by 0x65DEFC: avfilter_graph_parse2 (graphparser.c:431)
==30745==    by 0x4615D4: init_complex_filtergraph (ffmpeg_filter.c:353)
==30745==    by 0x42DB4B: init_complex_filters (ffmpeg_opt.c:2102)
==30745==    by 0x42DB4B: ffmpeg_parse_options (ffmpeg_opt.c:3324)
==30745==    by 0x487B43: main (ffmpeg.c:4862)
==30745==
==30745== LEAK SUMMARY:
==30745==    definitely lost: 32 bytes in 1 blocks
==30745==    indirectly lost: 0 bytes in 0 blocks
==30745==      possibly lost: 0 bytes in 0 blocks
==30745==    still reachable: 580 bytes in 15 blocks
==30745==         suppressed: 0 bytes in 0 blocks
==30745== Reachable blocks (those to which a pointer was found) are not shown.
==30745== To see them, rerun with: --leak-check=full --show-leak-kinds=all
==30745==
==30745== For counts of detected and suppressed errors, rerun with: -v
==30745== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
```

ASAN

```
=================================================================
==15214==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 32 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_asan+0x4de9e8)
    #1 0x8599368 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x8599368 in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x9397d2 in link_filter_inouts ffmpeg/libavfilter/graphparser.c:285:36
    #4 0x93620d in avfilter_graph_parse2 ffmpeg/libavfilter/graphparser.c:431:20
    #5 0x5850b4 in init_complex_filtergraph ffmpeg/fftools/ffmpeg_filter.c:353:11
    #6 0x516995 in init_complex_filters ffmpeg/fftools/ffmpeg_opt.c:2102:15
    #7 0x516995 in ffmpeg_parse_options ffmpeg/fftools/ffmpeg_opt.c:3324
    #8 0x5db156 in main ffmpeg/fftools/ffmpeg.c:4862:11
    #9 0x7f6e24c9cb96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../c

SUMMARY: AddressSanitizer: 32 byte(s) leaked in 1 allocation(s).
```

Please confirm.
Thanks

Attachments (1)

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

Change History (3)

by Suhwan, 3 years ago

Attachment: *PoC_graphparser.wav*added

comment:1 by Carl Eugen Hoyos, 3 years ago

Component:	undetermined → avfilter
Keywords:	leak added; valgrind asan removed
Priority:	normal → minor
Reproduced by developer:	set
Status:	new → open

comment:2 by mkver, 2 years ago

Component:	avfilter → ffmpeg
Resolution:	→ fixed
Status:	open → closed

Fixed in 426c16d61a9b5056a157a1a2a057a4e4d13eef84.

Note: See TracTickets for help on using tickets.