#8302 closed defect (fixed)

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

memory leaks in avi_add_ientry()

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

Description

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

```
% ffmpeg_g -y -i $PoC -filter_complex buffersink -c copy tmp.avi

ffmpeg version N-95441-g0ae6fb276b 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

```
==16010== HEAP SUMMARY:
==16010==     in use at exit: 262,184 bytes in 3 blocks
==16010==   total heap usage: 252 allocs, 249 frees, 2,009,670 bytes allocated
==16010==
==16010== 262,152 (8 direct, 262,144 indirect) bytes in 1 blocks are definitely lo
==16010==    at 0x9FE0A3F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-l
==16010==    by 0x9FE2D84: realloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
==16010==    by 0x592E631: av_realloc (mem.c:144)
==16010==    by 0x592E631: av_realloc_f (mem.c:157)
==16010==    by 0x146737C: avi_add_ientry (avienc.c:117)
==16010==    by 0x1466ABB: avi_write_packet_internal (avienc.c:893)
==16010==    by 0x146226F: avi_write_packet (avienc.c:853)
==16010==    by 0x17E6344: write_packet (mux.c:747)
==16010==    by 0x17ECD05: av_interleaved_write_frame (mux.c:1238)
==16010==    by 0x4B5DEA: write_packet (ffmpeg.c:815)
==16010==    by 0x4A3F70: do_streamcopy (ffmpeg.c:0)
==16010==    by 0x4A3F70: process_input_packet (ffmpeg.c:2736)
==16010==    by 0x4BF0EF: process_input (ffmpeg.c:4508)
==16010==    by 0x48D5EA: transcode_step (ffmpeg.c:4628)
==16010==    by 0x48D5EA: transcode (ffmpeg.c:4682)
==16010==
==16010== LEAK SUMMARY:
==16010==    definitely lost: 8 bytes in 1 blocks
==16010==    indirectly lost: 262,144 bytes in 1 blocks
==16010==      possibly lost: 0 bytes in 0 blocks
==16010==    still reachable: 32 bytes in 1 blocks
==16010==         suppressed: 0 bytes in 0 blocks
==16010== Reachable blocks (those to which a pointer was found) are not shown.
==16010== To see them, rerun with: --leak-check=full --show-leak-kinds=all
==16010==
==16010== For counts of detected and suppressed errors, rerun with: -v
==16010== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
```

Please confirm.
Thanks

Attachments (1)

- PoC_avi_add.pct(675.8 KB) - added by Suhwan 3 years ago.
  poc

Change History (3)

by Suhwan, 3 years ago

Attachment: *PoC_avi_add.pct*added

poc

comment:1 by James, 3 years ago

Component: undetermined → avformat
Resolution: → fixed
Status: new → closed

Fixed in a581bb66ea5eb981e2e498ca301df7d1ef15a6a3

comment:2 by Carl Eugen Hoyos, 3 years ago

Keywords: avi leak added
Priority: important → normal

Note: See TracTickets for help on using tickets.