#8282 closed defect (fixed)

Opened 3 years ago
Closed 3 years ago

invalid free at at libavfilter/avfilter.c:771

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

Description

Summary of the bug:
There is an invalid free at libavutil/dict.c:209
How to reproduce:

```
% ffmpeg_g -y -i $PoC -filter_complex gblur -target dv50 -loglevel 0 tmp.fsb

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

Here's GDB log

```
free(): invalid next size (fast)

Thread 1 "ffmpeg_g" received signal SIGABRT, Aborted.
__GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
51      ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) bt
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
#1  0x00007ffff5cb2801 in __GI_abort () at abort.c:79
#2  0x00007ffff5cfb897 in __libc_message (action=action@entry=do_abort,
    fmt=fmt@entry=0x7ffff5e28b9a "%s\n") at ../sysdeps/posix/libc_fatal.c:181
#3  0x00007ffff5d0290a in malloc_printerr (
    str=str@entry=0x7ffff5e2a800 "free(): invalid next size (fast)") at malloc.c:5
#4  0x00007ffff5d09f60 in _int_free (have_lock=0, p=0x9132d50, av=0x7ffff605dc40 <
    at malloc.c:4213
#5  __GI___libc_free (mem=0x9132d60) at malloc.c:3124
#6  0x000000000058ca92f in av_dict_free (pm=0x7fffffffbfa8) at libavutil/dict.c:209
#7  0x000000000591bfld in av_opt_set_dict2 (obj=0x93048c0, options=<optimized out>
    at libavutil/opt.c:1621
#8  0x000000000344a249 in avcodec_open2 (avctx=0x9304440, codec=0x6d47b10 <ff_dvvi
    options=<optimized out>) at libavcodec/utils.c:640
#9  0x00000000021540d9 in ff_frame_thread_encoder_init (avctx=0x9111c40, options=0
    at libavcodec/frame_thread_encoder.c:220
#10 0x000000000344d160 in avcodec_open2 (avctx=0x9111c40, codec=0x6d47b10 <ff_dvvi
    options=<optimized out>) at libavcodec/utils.c:740
#11 0x00000000004a67f2 in init_output_stream (ost=<optimized out>, error=<optimize
    error_len=1024) at fftools/ffmpeg.c:3507
#12 0x00000000004bff96 in reap_filters (flush=0) at fftools/ffmpeg.c:1442
#13 0x0000000000048d612 in transcode_step () at fftools/ffmpeg.c:4638
#14 transcode () at fftools/ffmpeg.c:4682
#15 0x0000000000487d54 in main (argc=11, argv=<optimized out>) at fftools/ffmpeg.c
```

ASAN log

```
==20551==ERROR: AddressSanitizer: attempting free on address which was not malloc(
    #0 0x4ddbe0 in __interceptor_free.localalias.0 (ffmpeg_asan+0x4ddbe0)
    #1 0x81a8f7 in avfilter_free ffmpeg/libavfilter/avfilter.c:771:9
    #2 0x835347 in avfilter_graph_free ffmpeg/libavfilter/avfiltergraph.c:126:9
    #3 0x5dbdf9 in ffmpeg_cleanup ffmpeg/fftools/ffmpeg.c:494:9
    #4 0x5afb04 in exit_program ffmpeg/fftools/cmdutils.c:139:9
    #5 0x5db8e2 in main ffmpeg/fftools/ffmpeg.c:4901:5
    #6 0x7ffff5c93b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../c
    #7 0x41def9 in _start (ffmpeg_asan+0x41def9)

0x60900000a840 is located 0 bytes inside of 97902940-byte region [0x60900000a840,0
==20551==AddressSanitizer CHECK failed: /build/llvm-toolchain-6.0-QjOn7h/llvm-tool
    #0 0x4e6f05 in __asan::AsanCheckFailed(char const*, int, char const*, unsigned
    #1 0x5047b5 in __sanitizer::CheckFailed(char const*, int, char const*, unsigne
    #2 0x42cc4c in __asan::HeapAddressDescription::Print() const (ffmpeg_asan+0x42
    #3 0x42e1bb in __asan::ErrorFreeNotMalloced::Print() (ffmpeg_asan+0x42e1bb)
    #4 0x4e46a3 in __asan::ReportFreeNotMalloced(unsigned long, __sanitizer::Buffe
    #5 0x42941f in __asan::asan_free(void*, __sanitizer::BufferedStackTrace*, __as
    #6 0x4ddbba in __interceptor_free.localalias.0 (ffmpeg_asan+0x4ddbba)
    #7 0x81a8f7 in avfilter_free ffmpeg/libavfilter/avfilter.c:771:9
    #8 0x835347 in avfilter_graph_free ffmpeg/libavfilter/avfiltergraph.c:126:9
    #9 0x5dbdf9 in ffmpeg_cleanup ffmpeg/fftools/ffmpeg.c:494:9
    #10 0x5afb04 in exit_program ffmpeg/fftools/cmdutils.c:139:9
    #11 0x5db8e2 in main ffmpeg/fftools/ffmpeg.c:4901:5
    #12 0x7ffff5c93b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../
    #13 0x41def9 in _start (ffmpeg_asan+0x41def9)
```

Attachments (1)

- PoC_dict_209.png48(290 bytes) - added by Suhwan 3 years ago.
  poc

Change History (3)

by Suhwan, 3 years ago

Attachment: *PoC_dict_209.png48*added

poc

comment:1 by Suhwan, 3 years ago

Summary: invalid free at libavutil/dict.c:209 → invalid free at at libavfilter/avfilter.c:771

```
ffmpeg version N-95389-gdd01947397 Copyright (c) 2000-2019 the FFmpeg developers
built with clang version 6.0.0-1ubuntu2 (tags/RELEASE_600/final)
```

```
free(): invalid size

Thread 1 "ffmpeg_g" received signal SIGABRT, Aborted.
```

```
__GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
51      ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) bt
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
#1  0x00007ffff5cb2801 in __GI_abort () at abort.c:79
#2  0x00007ffff5cfb897 in __libc_message (action=action@entry=do_abort, fmt=fmt@enti
#3  0x00007ffff5d0290a in malloc_printerr (str=str@entry=0x7ffff5e26da0 "free(): inv
#4  0x00007ffff5d09e2c in _int_free (have_lock=0, p=0x914a6f0, av=0x0) at malloc.c:4
#5  __GI___libc_free (mem=0x914a700) at malloc.c:3124
#6  0x00000000005ca023 in avfilter_free (filter=0x9148440) at libavfilter/avfilter.c
#7  0x00000000005d5fd8 in avfilter_graph_free (graph=0x910b710) at libavfilter/avfil
#8  0x000000000048814b in ffmpeg_cleanup (ret=0) at fftools/ffmpeg.c:494
#9  0x0000000000474463 in exit_program (ret=0) at fftools/cmdutils.c:139
#10 0x0000000000487eef in main (argc=<optimized out>, argv=<optimized out>) at fftoo
```

comment:2 by Elon Musk, 3 years ago

Resolution: → fixed

Status: new → closed

Note: See TracTickets for help on using tickets.