#8250 closed defect (fixed)

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

heap-buffer-overflow at libavfilter/vf_colorconstancy.c:282

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

Description

Summary of the bug:
There is a heap-buffer-overflow at libavfilter/vf_colorconstancy.c:282 in slice_get_derivative
I compiled ffmpeg with "--toolchain=clang-asan" to check the memory corruption and attached log file.

How to reproduce:

```
% ffmpeg_g -t 2 -y -r 38 -i $PoC -filter_complex greyedge -target dv -loglevel 99

ffmpeg version N-95314-g1331e00179 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 --toolchain=clan
```

Here's ASAN log

```
=================================================================
==35623==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60a000000a38 a
READ of size 8 at 0x60a000000a38 thread T1
    #0 0xb2885b in slice_get_derivative ffmpeg/libavfilter/vf_colorconstancy.c:282
    #1 0x9429d9 in worker_func ffmpeg/libavfilter/pthread.c:50:15
    #2 0x8658de2 in run_jobs ffmpeg/libavutil/slicethread.c:61:9
    #3 0x865674d in thread_worker ffmpeg/libavutil/slicethread.c:85:13
    #4 0x4eb9de in __asan::AsanThread::ThreadStart(unsigned long, __sanitizer::ato
    #5 0x7ffff668e6da in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x76d
    #6 0x7ffff5d9388e in clone /build/glibc-OTsEL5/glibc-2.27/misc/../sysdeps/unix

0x60a000000a38 is located 8 bytes to the left of 56-byte region [0x60a000000a40,0x
allocated by thread T0 here:
    #0 0x4de9e8 in posix_memalign (ffmpeg/ffmpeg_g+0x4de9e8)
    #1 0x8565daa in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x8565daa in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x8565daa in av_mallocz_array ffmpeg/libavutil/mem.c:195
    #4 0xb1cdc0 in set_gauss ffmpeg/libavfilter/vf_colorconstancy.c:119:23
    #5 0xb1cdc0 in config_props ffmpeg/libavfilter/vf_colorconstancy.c:666

Thread T1 created by T0 here:
    #0 0x436f80 in pthread_create (ffmpeg/ffmpeg_g+0x436f80)
    #1 0x8655939 in avpriv_slicethread_create ffmpeg/libavutil/slicethread.c:147:1

SUMMARY: AddressSanitizer: heap-buffer-overflow ffmpeg/libavfilter/vf_colorconstan
```

Please confirm.
Thanks

Attachments (2)

- gdb-vf_colorconstancy_282(15.0 KB) - added by Suhwan 3 years ago.
- PoC_vf_colorconstancy_282.bmp(14.2 KB) - added by Suhwan 3 years ago.
  poc

Change History (4)

by Suhwan, 3 years ago

Attachment: *gdb-vf_colorconstancy_282*added

by Suhwan, 3 years ago

Attachment: *PoC_vf_colorconstancy_282.bmp*added

poc

comment:1 by Elon Musk, 3 years ago

Resolution: → fixed
Status: new → closed

comment:2 by Carl Eugen Hoyos, 3 years ago

Component: undetermined → avfilter
Keywords: colorconstancy added

a7fd1279703683ebb548ef7baa2f1519994496ae

Note: See TracTickets for help on using tickets.