#8309 closed defect (fixed)

Opened 3 years ago
Closed 3 years ago

heap-buffer-overflow at libavfilter/drawutils.c:341

Reported by:	Suhwan	Owned by:	
Priority:	important	Component:	undetermined
Version:	git-master	Keywords:	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/drawutils.c:341 in ff_fill_rectangle

I compiled ffmpeg with "--toolchain=clang-asan" to check the memory corruption and attached log file.
How to reproduce:

```
% ffmpeg_g -y -i $PoC  -filter_complex oscilloscope tmp.mp3

ffmpeg version N-95450-g1d479300cb 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

```
=================================================================
==8790==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x611000001180 at
WRITE of size 4 at 0x611000001180 thread T0
    #0 0x4dcadb in __asan_memcpy (ffmpeg_g+0x4dcadb)
    #1 0x1b12aad in ff_fill_rectangle ffmpeg/libavfilter/drawutils.c:341:13
    #2 0xbdb58b in oscilloscope_filter_frame ffmpeg/libavfilter/vf_datascope.c:981
    #3 0x827129 in ff_filter_activate_default ffmpeg/libavfilter/avfilter.c:1084:1
    #4 0x827129 in ff_filter_activate ffmpeg/libavfilter/avfilter.c:1443
    #5 0x86ffd5 in push_frame ffmpeg/libavfilter/buffersrc.c:187:15
    #6 0x86ffd5 in av_buffersrc_add_frame_internal ffmpeg/libavfilter/buffersrc.c:
    #7 0x86ea62 in av_buffersrc_add_frame_flags ffmpeg/libavfilter/buffersrc.c:170
    #8 0x666467 in ifilter_send_frame ffmpeg/fftools/ffmpeg.c:2186:11
    #9 0x666467 in send_frame_to_filters ffmpeg/fftools/ffmpeg.c:2260
    #10 0x6076c6 in decode_video ffmpeg/fftools/ffmpeg.c:2459:11
    #11 0x6076c6 in process_input_packet ffmpeg/fftools/ffmpeg.c:2613
    #12 0x64a767 in process_input ffmpeg/fftools/ffmpeg.c:4508:5
    #13 0x5e71b7 in transcode_step ffmpeg/fftools/ffmpeg.c:4628:11
    #14 0x5e71b7 in transcode ffmpeg/fftools/ffmpeg.c:4682
    #15 0x5db6bb in main ffmpeg/fftools/ffmpeg.c:4884:9
    #16 0x7fb30df9cb96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../
    #17 0x41def9 in _start (ffmpeg_g+0x41def9)

0x611000001180 is located 64 bytes to the left of 143-byte region [0x6110000011c0,
allocated by thread T0 here:
    #0 0x4de9e8 in posix_memalign (ffmpeg_g+0x4de9e8)
    #1 0x85c4251 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x852b181 in av_buffer_alloc ffmpeg/libavutil/buffer.c:72:12
    #3 0x852b181 in av_buffer_allocz ffmpeg/libavutil/buffer.c:85
    #4 0x852f9a6 in pool_alloc_buffer ffmpeg/libavutil/buffer.c:313:26
    #5 0x852f9a6 in av_buffer_pool_get ffmpeg/libavutil/buffer.c:349
    #6 0x2ef33d2 in video_get_buffer ffmpeg/libavcodec/decode.c:1678:23
    #7 0x2ef33d2 in avcodec_default_get_buffer2 ffmpeg/libavcodec/decode.c:1717
    #8 0x2efaedc in get_buffer_internal ffmpeg/libavcodec/decode.c:1945:11
    #9 0x2efaedc in ff_get_buffer ffmpeg/libavcodec/decode.c:1970

SUMMARY: AddressSanitizer: heap-buffer-overflow (ffmpeg_g+0x4dcadb) in __asan_memc
Shadow bytes around the buggy address:
  0x0c227fff81e0: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c227fff81f0: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa fa fa
  0x0c227fff8200: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8210: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c227fff8220: 00 00 fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c227fff8230:[fa]fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c227fff8240: 00 00 00 00 00 00 00 00 00 07 fa fa fa fa fa fa
  0x0c227fff8250: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8260: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c227fff8270: 00 00 00 fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8280: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==8790==ABORTING
```

Please confirm.
Thanks

Attachments (1)

- PoC.pfa(146 bytes) - added by Suhwan 3 years ago.
  poc

Change History (2)

by Suhwan, 3 years ago

Attachment: *PoC.pfa*added

poc

comment:1 by Elon Musk, 3 years ago

- Resolution: → fixed
- Status: new → closed

Note: See TracTickets for help on using tickets.