#8275 closed defect (fixed)

Opened 3 years ago
Closed 3 years ago

heap-buffer-overflow at libavfilter/vf_edgedetect.c:180 in gaussian_blur

Reported by:	Suhwan	Owned by:	
Priority:	normal	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/vf_edgedetect.c:180 in gaussian_blur

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 edgedetect -target dv tmp.daud

ffmpeg version N-95382-g62f4722582 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

```
==47511==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61500001bee2 a
WRITE of size 1 at 0x61500001bee2 thread T0
    #0 0xcd9f0d in gaussian_blur ffmpeg/libavfilter/vf_edgedetect.c:180:20
    #1 0xcd9f0d in filter_frame ffmpeg/libavfilter/vf_edgedetect.c:364
    #2 0x8271b9 in ff_filter_activate_default ffmpeg/libavfilter/avfilter.c:1084:1
    #3 0x8271b9 in ff_filter_activate ffmpeg/libavfilter/avfilter.c:1443
    #4 0x8700b2 in push_frame ffmpeg/libavfilter/buffersrc.c:187:15
    #5 0x8700b2 in av_buffersrc_add_frame_internal ffmpeg/libavfilter/buffersrc.c:
    #6 0x86eaf2 in av_buffersrc_add_frame_flags ffmpeg/libavfilter/buffersrc.c:170
    #7 0x666407 in ifilter_send_frame ffmpeg/fftools/ffmpeg.c:2186:11
    #8 0x666407 in send_frame_to_filters ffmpeg/fftools/ffmpeg.c:2260
    #9 0x607666 in decode_video ffmpeg/fftools/ffmpeg.c:2459:11
    #10 0x607666 in process_input_packet ffmpeg/fftools/ffmpeg.c:2613
    #11 0x644c58 in process_input ffmpeg/fftools/ffmpeg.c:4303:23
    #12 0x5e7157 in transcode_step ffmpeg/fftools/ffmpeg.c:4628:11
    #13 0x5e7157 in transcode ffmpeg/fftools/ffmpeg.c:4682
    #14 0x5db65b in main ffmpeg/fftools/ffmpeg.c:4884:9
    #15 0x7ffff5c93b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../
    #16 0x41def9 in _start (ffmpeg_asan+0x41def9)

0x61500001bee2 is located 0 bytes to the right of 418-byte region [0x61500001bd40,
allocated by thread T0 here:
    #0 0x4de9e8 in posix_memalign (ffmpeg_asan+0x4de9e8)
    #1 0x85924d1 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0xcda91c in config_props ffmpeg/libavfilter/vf_edgedetect.c:137:29

SUMMARY: AddressSanitizer: heap-buffer-overflow ffmpeg/libavfilter/vf_edgedetect.c
Shadow bytes around the buggy address:
  0x0c2a7fffb780: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a7fffb790: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a7fffb7a0: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c2a7fffb7b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fffb7c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c2a7fffb7d0: 00 00 00 00 00 00 00 00 00 00 00 00[02]fa fa fa
  0x0c2a7fffb7e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a7fffb7f0: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c2a7fffb800: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fffb810: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fffb820: 00 00 00 00 00 00 00 00 00 00 00 00 02 fa fa fa
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
==47511==ABORTING
```

Please confirm.
Thanks

Attachments (1)

- PoC_vf_edgedetect_180.png(423 bytes) - added by Suhwan 3 years ago.
  poc

Change History (2)

by Suhwan, 3 years ago

Attachment: *PoC_vf_edgedetect_180.png*added

poc

comment:1 by Elon Musk, 3 years ago

Resolution: → fixed
Status: new → closed

Note: See TracTickets for help on using tickets.