#8274 closed defect (fixed)

Opened 3 years ago
Closed 3 years ago

heap-buffer-overflow at libavfilter/vf_avgblur.c:172

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/vf_avgblur.c:172 in filter_vertically_8
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 avgblur -target dv50 -loglevel 99 tmp.acm

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

```
=================================================================
==6091==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x609000006c50 at
READ of size 4 at 0x609000006c50 thread T1
    #0 0x9a5199 in filter_vertically_8 ffmpeg/libavfilter/vf_avgblur.c:172:1
    #1 0x942909 in worker_func ffmpeg/libavfilter/pthread.c:50:15
    #2 0x86863a2 in run_jobs ffmpeg/libavutil/slicethread.c:61:9
    #3 0x8683d0d 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

0x609000006c50 is located 0 bytes to the right of 16-byte region [0x609000006c40,0
allocated by thread T0 here:
    #0 0x4de9e8 in posix_memalign (ffmpeg_asan+0x4de9e8)
    #1 0x8592f19 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x8592f19 in av_malloc_array ffmpeg/libavutil/mem.c:188
    #3 0x9a0bf3 in config_input ffmpeg/libavfilter/vf_avgblur.c:188:17

Thread T1 created by T0 here:
    #0 0x436f80 in pthread_create (ffmpeg_asan+0x436f80)
    #1 0x8682ef9 in avpriv_slicethread_create ffmpeg/libavutil/slicethread.c:147:1

SUMMARY: AddressSanitizer: heap-buffer-overflow ffmpeg/libavfilter/vf_avgblur.c:17
Shadow bytes around the buggy address:
  0x0c127fff8d30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c127fff8d40: 00 fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c127fff8d50: 00 00 00 fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c127fff8d60: 00 fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c127fff8d70: 00 00 00 fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c127fff8d80: fa fa fa fa fa fa fa fa 00 00[fa]fa fa fa fa fa
  0x0c127fff8d90: fa fa fa fa fa fa fa fa fd fa fa fa fa fa fa fa
  0x0c127fff8da0: fa fa fa fa fa fa fa fa fd fa fa fa fa fa fa fa
  0x0c127fff8db0: fa fa fa fa fa fa fa fa fd fa fa fa fa fa fa fa
  0x0c127fff8dc0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c127fff8dd0: 00 00 fa fa fa fa fa fa fa fa fa fa fa 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
==6091==ABORTING
```

Please confirm.
Thanks

Attachments (1)

- PoC_vf_avgblur_172.bmp(126 bytes) - added by Suhwan 3 years ago.
  poc

Change History (2)

by Suhwan, 3 years ago

Attachment: *PoC_vf_avgblur_172.bmp*added

poc

comment:1 by Elon Musk, 3 years ago

Resolution: → fixed
Status: new → closed

Note: See TracTickets for help on using tickets.