#8190 closed defect (fixed)

Opened 3 years ago
Closed 19 months ago

heap-buffer-overflow from libavformat/movenc.c

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

Description

Summary of the bug:
There is heap-buffer-overflow from libavformat/movenc.c:2049:28 in mov_write_video_tag due to the out of bounds in libavformat/movenc.c:2049

```
libavformat/movenc.c:2049:28: runtime error: index 256 out of bounds for type 'uin
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior libavformat/movenc.c:2049:

==28470==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x621000004f30 a
READ of size 4 at 0x621000004f30 thread T0
    #0 0x21b9776 in mov_write_video_tag ffmpeg/libavformat/movenc.c:2049:28
    #1 0x2197fff in mov_write_stsd_tag ffmpeg/libavformat/movenc.c:2269:15
    #2 0x2197fff in mov_write_stbl_tag ffmpeg/libavformat/movenc.c:2490
    #3 0x21866e4 in mov_write_minf_tag ffmpeg/libavformat/movenc.c:2757:16
    #4 0x21866e4 in mov_write_mdia_tag ffmpeg/libavformat/movenc.c:2811
    #5 0x21866e4 in mov_write_trak_tag ffmpeg/libavformat/movenc.c:3187
    #6 0x217f127 in mov_write_moov_tag ffmpeg/libavformat/movenc.c:4012:23
    #7 0x2159a98 in mov_write_trailer ffmpeg/libavformat/movenc.c
    #8 0x23269ac in av_write_trailer ffmpeg/libavformat/mux.c:1283:15
    #9 0x5ee7e0 in transcode ffmpeg/fftools/ffmpeg.c:4726:20
    #10 0x5db6eb in main ffmpeg/fftools/ffmpeg.c:4894:9
    #11 0x7fb4ca6d0b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../
    #12 0x41df89 in _start (ffmpeg_g+0x41df89)

0x621000004f30 is located 0 bytes to the right of 4656-byte region [0x621000003d00
allocated by thread T0 here:
    #0 0x4dea78 in posix_memalign (ffmpeg_g+0x4dea78)
    #1 0x852e9ea in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x852e9ea in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x852e9ea in av_mallocz_array ffmpeg/libavutil/mem.c:195
    #4 0x215ea7c in mov_init ffmpeg/libavformat/movenc.c:6245:19
    #5 0x230591f in avformat_init_output ffmpeg/libavformat/mux.c:418:20
    #6 0x2309ece in avformat_write_header ffmpeg/libavformat/mux.c:515:20

SUMMARY: AddressSanitizer: heap-buffer-overflow ffmpeg/libavformat/movenc.c:2049:2
```

How to reproduce:

```
% ./ffmpeg_g -t 3 -stream_loop 2 -y -i screen_codec.wmv -loglevel 0 -map 0 -c copy

ffmpeg version N-94982-gea673a0edb 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=cl
```

Attachments (1)

- screen_codec.wmv(959.9 KB) - added by Suhwan 3 years ago.
  poc

Change History (3)

by Suhwan, 3 years ago

Attachment: *screen_codec.wmv*added

poc

comment:1 by Michael Niedermayer, 19 months ago

Will submit a patch to ffmpeg-devel

comment:2 by Michael Niedermayer, 19 months ago

Resolution: → fixed
Status: new → closed

Patch here: https://lists.ffmpeg.org/pipermail/ffmpeg-devel/2021-May/280738.html
will apply the patch soon

Note: See TracTickets for help on using tickets.