Opened 2 years ago
Closed 2 years ago

#8860 closed defect (duplicate)

A stack-buffer-overflow in aacdec_template.c:539:24

Reported by:	Zhou Anshunkang	Owned by:	
Priority:	normal	Component:	avcodec
Version:	git-master	Keywords:	aac
Cc:		Blocked By:	
Blocking:		Reproduced by developer:	no
Analyzed by developer:	no		

Description

System info

Ubuntu x86_64, clang 6.0, ffmpeg (git-master https://github.com/FFmpeg/FFmpeg/commit/01a580f141627cfc8eae5de2300d2d93911887e3)

Configure

```
./configure --toolchain=clang-asan && make ffmpeg_g
```

Command line

```
./ffmpeg_g -y -f mov /dev/null -i @@
```

AddressSanitizer

```
 built with clang version 6.0.0-1ubuntu2 (tags/RELEASE_600/final)
  configuration: --disable-shared --enable-debug=3 --disable-ffplay --disable-ffpr
  libavutil      56. 58.100 / 56. 58.100
  libavcodec     58.101.100 / 58.101.100
  libavformat    58. 51.100 / 58. 51.100
  libavdevice    58. 11.101 / 58. 11.101
  libavfilter     7. 87.100 /  7. 87.100
  libswscale      5.  8.100 /  5.  8.100
  libswresample   3.  8.100 /  3.  8.100
[aac @ 0x61b000000080] Format aac detected only with low score of 1, misdetection 
[aac @ 0x61b000000080] Packet corrupt (stream = 0, dts = NOPTS).
[aac @ 0x619000000580] Error decoding AAC frame header.
[aac @ 0x619000000580] More than one AAC RDB per ADTS frame is not implemented. Up
[aac @ 0x619000000580] Multiple frames in a packet.
[aac @ 0x619000000580] channel element 3.6 is not allocated
[aac @ 0x61b000000080] decoding for stream 0 failed
[aac @ 0x61b000000080] Estimating duration from bitrate, this may be inaccurate
[aac @ 0x61b000000080] Could not find codec parameters for stream 0 (Audio: aac (M
Consider increasing the value for the 'analyzeduration' (0) and 'probesize' (50000
Input #0, aac, from '/home/seviezhou/stack-overflow-output_configure-aacdec_templa
  Duration: 00:00:00.02, bitrate: 198 kb/s
    Stream #0:0: Audio: aac (Main), 4.0, fltp, 198 kb/s
Stream mapping:
  Stream #0:0 -> #0:0 (aac (native) -> aac (native))
Press [q] to stop, [?] for help
[aac @ 0x619000001e80] Error decoding AAC frame header.
Error while decoding stream #0:0: Error number -50531338 occurred
[aac @ 0x619000001e80] Gain control is not implemented. Update your FFmpeg version
[aac @ 0x619000001e80] Sample rate index in program config element does not match 
=================================================================
==66288==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffeac79c4b4 
READ of size 1 at 0x7ffeac79c4b4 thread T0
    #0 0x27df270 in output_configure /home/seviezhou/ffmpeg/libavcodec/aacdec_temp
    #1 0x27ef51c in aac_decode_frame_int /home/seviezhou/ffmpeg/libavcodec/aacdec_
    #2 0x27d7843 in aac_decode_frame /home/seviezhou/ffmpeg/libavcodec/aacdec_temp
    #3 0x12659b8 in decode_simple_internal /home/seviezhou/ffmpeg/libavcodec/decod
    #4 0x12659b8 in decode_simple_receive_frame /home/seviezhou/ffmpeg/libavcodec/
    #5 0x12659b8 in decode_receive_frame_internal /home/seviezhou/ffmpeg/libavcode
    #6 0x12652cd in avcodec_send_packet /home/seviezhou/ffmpeg/libavcodec/decode.c
    #7 0x567e4e in decode /home/seviezhou/ffmpeg/fftools/ffmpeg.c:2217:15
    #8 0x567e4e in decode_audio /home/seviezhou/ffmpeg/fftools/ffmpeg.c:2274
    #9 0x567e4e in process_input_packet /home/seviezhou/ffmpeg/fftools/ffmpeg.c:25
    #10 0x560528 in process_input /home/seviezhou/ffmpeg/fftools/ffmpeg.c:4493:5
    #11 0x560528 in transcode_step /home/seviezhou/ffmpeg/fftools/ffmpeg.c:4613
    #12 0x560528 in transcode /home/seviezhou/ffmpeg/fftools/ffmpeg.c:4667
    #13 0x555f45 in main /home/seviezhou/ffmpeg/fftools/ffmpeg.c:4872:9
    #14 0x7fb163d6db96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../
    #15 0x41df49 in _start (/home/seviezhou/ffmpeg/ffmpeg_g+0x41df49)

Address 0x7ffeac79c4b4 is located in stack of thread T0 at offset 1012 in frame
    #0 0x27ea7ef in aac_decode_frame_int /home/seviezhou/ffmpeg/libavcodec/aacdec_

  This frame has 7 object(s):
    [32, 288) 'buf.i.i' (line 2467)
    [352, 356) 'major.i.i' (line 2468)
    [368, 372) 'minor.i.i' (line 2468)
    [384, 404) 'hdr_info.i' (line 3065)
    [448, 640) 'layout_map.i' (line 3066)
    [704, 768) 'che_presence' (line 3206)
    [800, 992) 'layout_map' (line 3292) <== Memory access at offset 1012 overflows
HINT: this may be a false positive if your program uses some custom stack unwind m
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow /home/seviezhou/ffmpeg/libavcodec
Shadow bytes around the buggy address:
  0x1000558eb840: f2 f2 f2 f2 f8 f2 f8 f2 f8 f8 f8 f2 f2 f2 f2 f2
  0x1000558eb850: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8
  0x1000558eb860: f8 f8 f8 f8 f8 f8 f8 f8 f2 f2 f2 f2 f2 f2 f2 f2
  0x1000558eb870: 00 00 00 00 00 00 00 00 f2 f2 f2 f2 00 00 00 00
  0x1000558eb880: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x1000558eb890: 00 00 00 00 f3 f3[f3]f3 f3 f3 f3 f3 00 00 00 00
  0x1000558eb8a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000558eb8b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000558eb8c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000558eb8d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000558eb8e0: 00 00 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1
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
==66288==ABORTING
```

Attachm

- stack-overflow-output_configure-aacdec_template-539(423 bytes) - added by Zhou Anshunkang 2 years ago.
  stack-overflow-output_configure-aacdec_template-539

Change History (4)

by Zhou Anshunkang, 2 years ago

Attachment: *stack-overflow-output_configure-aacdec_template-539*added

stack-overflow-output_configure-aacdec_template-539

comment:1 by Carl Eugen Hoyos, 2 years ago in reply to: description

Replying to ~~seviezhou~~:

> ```
>  configuration: --disable-shared --enable-debug=3 --disable-ffplay --disable-ffpr
> ```

As said: Please use `./configure --toolchain=clang-asan && make ffmpeg_g` instead to make your reports more readable. And maybe wait with opening more aac related reports until the ones you opened are fixed.

comment:2 by Zhou Anshunkang, 2 years ago

Use `./configure --toolchain=clang-asan && make ffmpeg_g`:

```
ffmpeg version N-98802-g01a580f141 Copyright (c) 2000-2020 the FFmpeg developers
  built with clang version 6.0.0-1ubuntu2 (tags/RELEASE_600/final)
  configuration: --toolchain=clang-asan
  libavutil      56. 58.100 / 56. 58.100
  libavcodec     58.101.100 / 58.101.100
  libavformat    58. 51.100 / 58. 51.100
  libavdevice    58. 11.101 / 58. 11.101
  libavfilter     7. 87.100 /  7. 87.100
  libswscale      5.  8.100 /  5.  8.100
  libswresample   3.  8.100 /  3.  8.100
[aac @ 0x61b000000080] Format aac detected only with low score of 1, misdetection po
[aac @ 0x61b000000080] Packet corrupt (stream = 0, dts = NOPTS).
[aac @ 0x619000000580] Error decoding AAC frame header.
[aac @ 0x619000000580] More than one AAC RDB per ADTS frame is not implemented. Upda
[aac @ 0x619000000580] Multiple frames in a packet.
[aac @ 0x619000000580] channel element 3.6 is not allocated
[aac @ 0x61b000000080] decoding for stream 0 failed
[aac @ 0x61b000000080] Estimating duration from bitrate, this may be inaccurate
[aac @ 0x61b000000080] Could not find codec parameters for stream 0 (Audio: aac (Ma
Consider increasing the value for the 'analyzeduration' (0) and 'probesize' (5000000
Input #0, aac, from 'stack-overflow-output_configure-aacdec_template-539':
  Duration: 00:00:00.02, bitrate: 198 kb/s
    Stream #0:0: Audio: aac (Main), 4.0, fltp, 198 kb/s
Stream mapping:
  Stream #0:0 -> #0:0 (aac (native) -> aac (native))
Press [q] to stop, [?] for help
[aac @ 0x619000001e80] Error decoding AAC frame header.
Error while decoding stream #0:0: Error number -50531338 occurred
[aac @ 0x619000001e80] Gain control is not implemented. Update your FFmpeg version t
[aac @ 0x619000001e80] Sample rate index in program config element does not match th
=================================================================
==30448==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7fffe9040e65 at
READ of size 1 at 0x7fffe9040e65 thread T0
    #0 0x294ef90 in output_configure /home/seviezhou/ffmpeg/libavcodec/aacdec_templa
    #1 0x295ee10 in aac_decode_frame_int /home/seviezhou/ffmpeg/libavcodec/aacdec_te
    #2 0x2947523 in aac_decode_frame /home/seviezhou/ffmpeg/libavcodec/aacdec_templa
    #3 0x126db5c in decode_simple_internal /home/seviezhou/ffmpeg/libavcodec/decode
    #4 0x126db5c in decode_simple_receive_frame /home/seviezhou/ffmpeg/libavcodec/de
    #5 0x126db5c in decode_receive_frame_internal /home/seviezhou/ffmpeg/libavcodec/
    #6 0x126d46d in avcodec_send_packet /home/seviezhou/ffmpeg/libavcodec/decode.c:(
    #7 0x567e4e in decode /home/seviezhou/ffmpeg/fftools/ffmpeg.c:2217:15
    #8 0x567e4e in decode_audio /home/seviezhou/ffmpeg/fftools/ffmpeg.c:2274
    #9 0x567e4e in process_input_packet /home/seviezhou/ffmpeg/fftools/ffmpeg.c:259(
    #10 0x560528 in process_input /home/seviezhou/ffmpeg/fftools/ffmpeg.c:4493:5
    #11 0x560528 in transcode_step /home/seviezhou/ffmpeg/fftools/ffmpeg.c:4613
    #12 0x560528 in transcode /home/seviezhou/ffmpeg/fftools/ffmpeg.c:4667
    #13 0x555f45 in main /home/seviezhou/ffmpeg/fftools/ffmpeg.c:4872:9
    #14 0x7ffa992fbb96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../cs
    #15 0x41df89 in _start (/home/seviezhou/ffmpeg/ffmpeg_g+0x41df89)

Address 0x7fffe9040e65 is located in stack of thread T0 at offset 165 in frame
    #0 0x2946f3f in aac_decode_frame /home/seviezhou/ffmpeg/libavcodec/aacdec_templa

  This frame has 4 object(s):
    [32, 64) 'gb.i' (line 1113)
    [96, 128) 'gb' (line 3413)
    [160, 164) 'new_extradata_size' (line 3417) <== Memory access at offset 165 over
    [176, 180) 'jp_dualmono_size' (line 3421)
HINT: this may be a false positive if your program uses some custom stack unwind mec
                                                                                   c/a


  0x10007d200190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007d2001a0: 00 00 00 00 f3 f3 f3 f3 f3 f3 f3 f3 00 00 00 00
  0x10007d2001b0: 00 00 00 00 00 00 00 00 f1 f1 f1 f1 f8 f8 f8 f8
=>0x10007d2001c0: f2 f2 f2 f2 00 00 00 00 f2 f2 f2 f2[04]f2 04 f3
  0x10007d2001d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007d2001e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007d2001f0: 00 00 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1
  0x10007d200200: 04 f2 f8 f3 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007d200210: 00 00 00 00 00 00 00 00 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
==30448==ABORTING
```

comment:3 by Carl Eugen Hoyos, 2 years ago

Resolution: → duplicate
Status: new → closed

Fixed by Jan Ekström in d6f293353c94c7ce200f6e0975ae3de49787f91f

Note: See TracTickets for help on using tickets.