#7995 closed defect (duplicate)

Opened 3 years ago
Closed 19 months ago
Last modified 19 months ago

Division by zero at libavcodec/aacpsy.c:797:29

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

Description

Summary of the bug:
There's division by zero at libavcodec/aacpsy.c:797:29 and also this triggers heap buffer overflow
How to reproduce:

```
% ffmpeg_g -y -i tmp.flv -map 0 -c:v zmbv -c:s:3 ayuv -disposition:v:109 dpx -disp

ffmpeg version : N-94163-g664a27ea40
built with clang version 9.0.0
```

In the code, varible 'norm_fac' is zero.

```
795         if (pe < 1.15f * desired_pe) {
796             /* 6.6.1.3.6 "Final threshold modification by linearization" */
797             norm_fac = 1.0f / norm_fac;
798             for (w = 0; w < wi->num_windows*16; w += 16) {
799                 for (g = 0; g < num_bands; g++) {
800                     AacPsyBand *band = &pch->band[w+g];
801
802                     if (band->active_lines > 0.5f) {
803                         float delta_sfb_pe = band->norm_fac * norm_fac * delt
804                         float thr = band->thr;
805
806                         thr *= exp2f(delta_sfb_pe / band->active_lines);
807                         if (thr > coeffs[g].min_snr * band->energy && band->a
808                             thr = FFMAX(band->thr, coeffs[g].min_snr * band->
809                         band->thr = thr;
810                     }
811                 }
812             }
```

Attachments (2)

- gdb_log_7995(7.9 KB) - added by Suhwan 3 years ago.
- tmp.flv(428.8 KB) - added by Suhwan 3 years ago.

Change History (5)

by Suhwan, 3 years ago

Attachment: *gdb_log_7995*added

by Suhwan, 3 years ago

Attachment: *tmp.flv*added

comment:1 by Suhwan, 3 years ago

```
ffmpeg version N-94906-gcb8d6a4e3e 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=cla
  libavutil      56. 35.100 / 56. 35.100
  libavcodec     58. 56.101 / 58. 56.101
  libavformat    58. 32.104 / 58. 32.104
  libavdevice    58.  9.100 / 58.  9.100
  libavfilter     7. 58.102 /  7. 58.102
  libswscale      5.  6.100 /  5.  6.100
  libswresample   3.  6.100 /  3.  6.100
Input #0, flv, from 'tmp.flv':
  Metadata:
    encoder         : Lavf57.66.105
  Duration: 00:00:05.60, start: 0.000000, bitrate: 627 kb/s
    Stream #0:0: Audio: mp3, 48000 Hz, mono, fltp, 64 kb/s
    Stream #0:1: Video: flv1, yuv420p, 560x320, 200 kb/s, 30 fps, 30 tbr, 1k tbn
Stream mapping:
  Stream #0:0 -> #0:0 (mp3 (mp3float) -> aac (native))
  Stream #0:1 -> #0:1 (flv1 (flv) -> zmbv (native))
Press [q] to stop, [?] for help
[aac @ 0x9b19d40] Bitrate 945 is extremely low, maybe you mean 945k
[aac @ 0x9b19d40] Using a PCE to encode channel layout "2.1"
The bitrate parameter is set too low. It takes bits/s as argument, not kbits/s
Output #0, latm, to 'tmp_.loas':
  Metadata:
    encoder         : Lavf58.32.104
    Stream #0:0: Audio: aac (LC), 48000 Hz, 2.1, fltp, 0 kb/s
    Metadata:
      encoder         : Lavc58.56.101 aac
    Stream #0:1: Video: zmbv, bgr0, 560x320, q=2-31, 200 kb/s, 6 fps, 6 tbn, 6 tbc
    Metadata:
      encoder         : Lavc58.56.101 zmbv
libavcodec/aacpsy.c:797:29: runtime error: division by zero
[latm @ 0x9af9500] LATM packet size larger than maximum size 0x1fff=   1.8kbits/s s
av_interleaved_write_frame(): Invalid data found when processing input
[latm @ 0x9af9500] LATM packet size larger than maximum size 0x1fff
Error writing trailer of tmp_.loas: Invalid data found when processing input
frame=    2 fps=0.0 q=-0.0 Lsize=       0kB time=00:00:00.33 bitrate=   2.2kbits/s
video:291kB audio:0kB subtitle:0kB other streams:0kB global headers:0kB muxing overh
[aac @ 0x9b19d40] Qavg: 0.067
Conversion failed!
```

comment:2 by Michael Niedermayer, 19 months ago

Cc:	Michael Niedermayer added
Resolution:	→ duplicate
Status:	new → closed

The out of array access is a duplicate of ~~#7980~~
There is no integer division by 0. Floating point divisions by 0 is not a bug as such.

comment:3 by Michael Niedermayer, 19 months ago

I will post a patch to ffmpeg-devel to avoid the floating point division.

Note: See TracTickets for help on using tickets.