#8003 closed defect (fixed)

Opened 3 years ago
Closed 19 months ago

Division by zero at libavcodec/aaccoder.c

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

Description

Summary of the bug:
There's a division by zero at libavcodec/aaccoder.c:554 and 556.

How to reproduce:

```
% ffmpeg_g -y -r 14 -i tmp.wmv -map 0 -c:v:14 mpeg1video -c:v zmbv -disposition:s:

ffmpeg version N-94185-gca576833e4 Copyright (c) 2000-2019 the FFmpeg developers
built with clang version 9.0.0
```

s->lambda is zero.

```
543 static void search_for_pns(AACEncContext *s, AVCodecContext *avctx, SingleChan
544 {
545     FFPsyBand *band;
546     int w, g, w2, i;
547     int wlen = 1024 / sce->ics.num_windows;
548     int bandwidth, cutoff;
549     float *PNS = &s->scoefs[0*128], *PNS34 = &s->scoefs[1*128];
550     float *NOR34 = &s->scoefs[3*128];
551     uint8_t nextband[128];
552     const float lambda = s->lambda;
553     const float freq_mult = avctx->sample_rate*0.5f/wlen;
554     const float thr_mult = NOISE_LAMBDA_REPLACE*(100.0f/lambda);
555     const float spread_threshold = FFMIN(0.75f, NOISE_SPREAD_THRESHOLD*FFMAX(0
556     const float dist_bias = av_clipf(4.f * 120 / lambda, 0.25f, 4.0f);
557     const float pns_transient_energy_r = FFMIN(0.7f, lambda / 140.f);
```

Attachments (2)

- gdb_log_8003(8.2 KB) - added by Suhwan 3 years ago.
- tmp.wmv(444.8 KB) - added by Suhwan 3 years ago.

Change History (5)

by Suhwan, 3 years ago

Attachment: *gdb_log_8003*added

by Suhwan, 3 years ago

Attachment: *tmp.wmv*added

comment:1 by Suhwan, 3 years ago

FFmpeg Version: 4.2 (git master)
Many division by zero bugs are triggered.

```
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
Guessed Channel Layout for Input Stream #0.1 : mono
Input #0, asf, from 'tmp.wmv':
  Metadata:
    encoder         : Lavf57.66.105
  Duration: 00:00:05.63, start: 0.000000, bitrate: 647 kb/s
    Stream #0:0: Video: wmv2 (WMV2 / 0x32564D57), yuv420p, 560x320, SAR 1:1 DAR 7:4,
    Stream #0:1(eng): Audio: wmav2 (a[1][0][0] / 0x0161), 48000 Hz, mono, fltp, 128
Stream mapping:
  Stream #0:0 -> #0:0 (wmv2 (native) -> zmbv (native))
  Stream #0:1 -> #0:1 (wmav2 (native) -> aac (native))
Press [q] to stop, [?] for help
[aac @ 0x9399480] Bitrate 45 is extremely low, maybe you mean 45k
The bitrate parameter is set too low. It takes bits/s as argument, not kbits/s
libavcodec/aaccoder.c:554:56: runtime error: division by zero
libavcodec/aaccoder.c:556:48: runtime error: division by zero
[mov @ 0x9389400] Using MS style video codec tag, the file may be unplayable!
Output #0, mov, to 'tmp_.mov':
  Metadata:
    encoder         : Lavf58.32.104
    Stream #0:0: Video: zmbv, bgr0, 560x320 [SAR 1:1 DAR 7:4], q=2-31, 292 kb/s, 14
    Metadata:
      encoder         : Lavc58.56.101 zmbv
    Stream #0:1(eng): Audio: aac (LC) (mp4a / 0x6134706D), 48000 Hz, mono, fltp, 0
    Metadata:
      encoder         : Lavc58.56.101 aac
frame=  166 fps=6.0 q=-0.0 Lsize=    9258kB time=00:00:11.78 bitrate=6434.9kbits/s
video:9255kB audio:0kB subtitle:0kB other streams:0kB global headers:0kB muxing ove
[aac @ 0x9399480] Qavg: 0.000
```

Last edited 3 years ago by Suhwan (previous) (diff)

comment:2 by Michael Niedermayer, 19 months ago

Patch avoiding the floating point divisions by 0 is on the ffmpeg-devel mailing list.
https://lists.ffmpeg.org/pipermail/ffmpeg-devel/2021-May/280730.html
How this would allow a Denial of Service in reality is not clear.

comment:3 by Michael Niedermayer, 19 months ago

Resolution: → fixed
Status: new → closed

Fixed in a7a7f32c8ad0179a1a85d0a8cff35924e6d90be8

Note: See TracTickets for help on using tickets.