Opened 18 months ago
Closed 17 months ago

#9312 closed defect (fixed)

assertion failed in av_rescale_delta

Reported by:	dzj	Owned by:	
Priority:	important	Component:	undetermined
Version:	git-master	Keywords:	crash abort
Cc:	dzj	Blocked By:	
Blocking:		Reproduced by developer:	yes
Analyzed by developer:	no		

Description

Summary of the bug
there is an assertion failure at src/libavutil/mathematics.c, causing ffmpeg aborted.

System info
Ubuntu 18.04.5 LTS
clang version 10.0.0
ffmpeg version (git commit de8e6e67e7523e48bb27ac224a0b446df05e1640)
commit date:Wed Jun 30 09:34:09 2021

How to build

```
./configure --cc=clang --cxx=clang++ --ld=clang --enable-debug
make
```

How to reproduce

```
ffmpeg ffmpeg -y -i crash_input -c:v mpeg4 -c:a copy -f mp4 /dev/null
```

Gdb output

```
Assertion duration >= 0 failed at src/libavutil/mathematics.c:172

Thread 1 "ffmpeg_g" received signal SIGABRT, Aborted.
__GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
51      ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) bt
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
#1  0x00007ffff7248921 in __GI_abort () at abort.c:79
#2  0x00000000014689a5 in av_rescale_delta (in_tb=..., in_ts=<optimized out>, fs_t
#3  0x0000000000422647 in do_streamcopy (ist=0x22b4040, ost=0x22cab00, pkt=0x22b42
#4  process_input_packet (ist=<optimized out>, pkt=<optimized out>, no_eof=<optimi
#5  0x000000000041e4a6 in process_input (file_index=<optimized out>) at src/fftool
#6  transcode_step () at src/fftools/ffmpeg.c:4758
#7  transcode () at src/fftools/ffmpeg.c:4812
#8  0x000000000041a822 in main (argc=<optimized out>, argv=<optimized out>) at src
(gdb) disass $pc-32,$pc+32
Dump of assembler code from 0x7ffff7246f97 to 0x7ffff7246fd7:
   0x00007ffff7246f97 <__GI_raise+167>: add    %dh,%al
   0x00007ffff7246f99 <__GI_raise+169>: (bad)
   0x00007ffff7246f9a <__GI_raise+170>: pushq  0x3b(%rdi)
   0x00007ffff7246f9d <__GI_raise+173>: mov    %eax,%r8d
   0x00007ffff7246fa0 <__GI_raise+176>: mov    $0x8,%r10d
   0x00007ffff7246fa6 <__GI_raise+182>: xor    %edx,%edx
   0x00007ffff7246fa8 <__GI_raise+184>: mov    %r9,%rsi
   0x00007ffff7246fab <__GI_raise+187>: mov    $0x2,%edi
   0x00007ffff7246fb0 <__GI_raise+192>: mov    $0xe,%eax
   0x00007ffff7246fb5 <__GI_raise+197>: syscall
=> 0x00007ffff7246fb7 <__GI_raise+199>: mov    0x108(%rsp),%rcx
   0x00007ffff7246fbf <__GI_raise+207>: xor    %fs:0x28,%rcx
   0x00007ffff7246fc8 <__GI_raise+216>: mov    %r8d,%eax
   0x00007ffff7246fcb <__GI_raise+219>: jne    0x7ffff7246fec <__GI_raise+252>
   0x00007ffff7246fcd <__GI_raise+221>: add    $0x118,%rsp
   0x00007ffff7246fd4 <__GI_raise+228>: retq
   0x00007ffff7246fd5 <__GI_raise+229>: nopl   (%rax)
End of assembler dump.
(gdb) info all-registers
rax            0x0      0
rbx            0x22b4040        36388928
rcx            0x7ffff7246fb7   140737339748279
rdx            0x0      0
rsi            0x7fffffffcdc0   140737488342464
rdi            0x2      2
rbp            0x22cab00        0x22cab00
rsp            0x7fffffffcdc0   0x7fffffffcdc0
r8             0x0      0
r9             0x7fffffffcdc0   140737488342464
r10            0x8      8
r11            0x246    582
r12            0xffffe412       4294960146
r13            0x22b3b80        36387712
r14            0x22b4240        36389440
r15            0x22cc4c0        36488384
rip            0x7ffff7246fb7   0x7ffff7246fb7 <__GI_raise+199>
eflags         0x246    [ PF ZF IF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
gs             0x0      0
st0            0        (raw 0x00000000000000000000)
st1            0        (raw 0x00000000000000000000)
st2            0        (raw 0x00000000000000000000)
st3            0        (raw 0x00000000000000000000)
st4            0        (raw 0x00000000000000000000)
st5            0        (raw 0x00000000000000000000)
st6            0        (raw 0x00000000000000000000)
st7            0        (raw 0x00000000000000000000)
fctrl          0x37f    895
fstat          0x0      0
ftag           0xffff   65535
fiseg          0x0      0
fioff          0x0      0
foseg          0x0      0
fooff          0x0      0
fop            0x0      0
mxcsr          0x1fa0   [ PE IM DM ZM OM UM PM ]
bndcfgu        {raw = 0x0, config = {base = 0x0, reserved = 0x0, preserved = 0x0,
bndstatus      {raw = 0x0, status = {bde = 0x0, error = 0x0}}   {raw = 0x0, status
k0             0x0      0
k1             0x0      0
k2             0x0      0
k3             0x0      0
k4             0x0      0
k5             0x0      0
k6             0x0      0
k7             0x0      0
pkru           0x55555554       1431655764
zmm0           {v16_float = {0x0, 0x0, 0x0, 0x0, 0x0 <repeats 12 times>}, v8_doubl
```

```
    0xffff, 0xffff, 0xffff, 0xffff, 0x0 <repeats 24 times>}, v16_int32 = {0xffffff
    0xffffffffffffffffffffffffffffffff, 0x0, 0x0, 0x0}}
```

Attachm

- abort_bug_input(399.8 KB) - added by dzj 18 months ago.
  poc file

Change History (5)

by dzj, 18 months ago

Attachment: *abort_bug_input*added

poc file

comment:1 by dzj, 18 months ago

Version: unspecified → git-master

comment:2 by dzj, 18 months ago

Priority: normal → important

comment:3 by Carl Eugen Hoyos, 18 months ago

Component: avutil → undetermined
Keywords: crash abort added
Reproduced by developer: set
Status: new → open

```
$ ffmpeg -i abort_bug_input -vn -c:a copy -f null -
ffmpeg version N-102812-g9583e66ea0 Copyright (c) 2000-2021 the FFmpeg developers
  built with gcc 10 (SUSE Linux)
  configuration: --enable-gpl
  libavutil      57.  0.100 / 57.  0.100
  libavcodec     59.  3.100 / 59.  3.100
  libavformat    59.  4.100 / 59.  4.100
  libavdevice    59.  0.100 / 59.  0.100
  libavfilter     8.  0.103 /  8.  0.103
  libswscale      6.  0.100 /  6.  0.100
  libswresample   4.  0.100 /  4.  0.100
  libpostproc    56.  0.100 / 56.  0.100
st:0 has too large timebase, reducing
[avi @ 0x31fa740] crazy start time, iam scared, giving up
[avi @ 0x31fa740] sample size (4) != block align (16)
[avi @ 0x31fa740] Something went wrong during header parsing, tag ST[4][1] has size
[adpcm_ms @ 0x31fc9c0] Too many or invalid channels: 22050
[avi @ 0x31fa740] Failed to open codec in avformat_find_stream_info
[adpcm_ms @ 0x31fc9c0] Too many or invalid channels: 22050
[mpeg4 @ 0x31fbb00] time_increment_bits 0 is invalid in relation to the current bit
[mpeg4 @ 0x31fbb00] time_increment_bits set to 15 bits, based on bitstream analysis
[mpeg4 @ 0x31fbb00] Error, header damaged or not MPEG-4 header (f_code=0)
[mpeg4 @ 0x31fbb00] time_increment_bits 4 is invalid in relation to the current bit
[mpeg4 @ 0x31fbb00] time_increment_bits set to 15 bits, based on bitstream analysis
[mpeg4 @ 0x31fbb00] looks like this file was encoded with (divx4/(old)xvid/opendivx
[mpeg4 @ 0x31fbb00] Error, header damaged or not MPEG-4 header (f_code=0)
    Last message repeated 2 times
[avi @ 0x31fa740] Packet corrupt (stream = 0, dts = 81).
Input #0, avi, from 'abort_bug_input':
  Duration: 00:00:00.01, start: 0.000000, bitrate: 271968 kb/s
  Stream #0:0: Video: mpeg4 (DX50 / 0x30355844), yuv420p, 352x288, 9300.90 fps, 930
  Stream #0:1: Audio: adpcm_ms ([2][0][0][0] / 0x0002), 786432000 Hz, 22050 channel
Output #0, null, to 'pipe:':
  Metadata:
    encoder         : Lavf59.4.100
  Stream #0:0: Audio: adpcm_ms ([2][0][0][0] / 0x0002), 786432000 Hz, 22050 channel
Stream mapping:
  Stream #0:1 -> #0:0 (copy)
Press [q] to stop, [?] for help
Assertion duration >= 0 failed at libavutil/mathematics.c:172
Aborted (core dumped)
```

comment:4 by James, 17 months ago

Resolution: → fixed
Status: open → closed

Should be fixed in e01d306c647b5827102260b885faa223b646d2d1

Note: See TracTickets for help on using tickets.