#8863 closed defect (fixed)

Opened 2 years ago
Closed 2 years ago

null pointer reference

Reported by:	lys404	Owned by:	
Priority:	important	Component:	avcodec
Version:	git-master	Keywords:	aac crash SIGSEGV
Cc:		Blocked By:	
Blocking:		Reproduced by developer:	yes
Analyzed by developer:	no		

Description

Summary of the bug:
There're null pointer in libavutil/mem.c

How to reproduce:

```
% ffmpeg -i $PoC output
ffmpeg version
built on ffmpeg version N-98759-g1c7e55d Copyright (c) 2000-2020 the FFmpeg develo
  built with gcc 5.4.0 (Ubuntu 5.4.0-6ubuntu1~16.04.12) 20160609
  configuration: --prefix=./out --disable-stripping --enable-debug --cc=afl-gcc --
```

Error information

```
Program received signal SIGSEGV, Segmentation fault.
```

Here's debugging information

```
gdb-peda$ bt
#0  0x00000000038aaf2b in av_freep (arg=arg@entry=0x433f08b2c82f1376) at libavutil
#1  0x00000000004cde0d in ff_mdct_end (s=s@entry=0x433f08b2c82f1356) at libavcodec
#2  0x0000000000055def8 in ff_aac_sbr_ctx_close (sbr=0x433f08b2c8291c26) at libavco
#3  0x0000000002cf2f90 in che_configure (channels=<synthetic pointer>, id=0x0, typ
    at libavcodec/aacdec_template.c:152
#4  output_configure (ac=0x49bb200, layout_map=<optimized out>, tags=0x10, oc_type
    at libavcodec/aacdec_template.c:543
#5  0x0000000002cfef22 in aac_decode_frame_int (avctx=avctx@entry=0x49b8a00, data=
    got_frame_ptr=got_frame_ptr@entry=0x7fffffffd860, gb=gb@entry=0x7fffffffd7d0,
#6  0x0000000002d046b5 in aac_decode_frame (avctx=0x49b8a00, data=0x49baac0, got_f
    at libavcodec/aacdec_template.c:3457
#7  0x0000000001818f01 in decode_simple_internal (frame=<optimized out>, avctx=<op
#8  decode_simple_receive_frame (frame=<optimized out>, avctx=<optimized out>) at
#9  decode_receive_frame_internal (avctx=avctx@entry=0x49b8a00, frame=0x49baac0) a
#10 0x0000000000181bde8 in avcodec_send_packet (avctx=avctx@entry=0x49b8a00, avpkt=
#11 0x00000000014ff73d in try_decode_frame (s=s@entry=0x49b7480, st=st@entry=0x49b
    at libavformat/utils.c:3111
#12 0x0000000001526a5f in avformat_find_stream_info (ic=0x49b7480, options=0x49b80
#13 0x00000000005f9e4d in open_input_file (o=o@entry=0x7fffffffdf00, filename=<opt
#14 0x000000000060420f in open_files (l=0x49b7058, l=0x49b7058, open_file=0x5f2730
    at fftools/ffmpeg_opt.c:3303
#15 ffmpeg_parse_options (argc=argc@entry=0x4, argv=argv@entry=0x7fffffffe4a8) at
#16 0x00000000005dbbb7 in main (argc=argc@entry=0x4, argv=argv@entry=0x7fffffffe4a
#17 0x00007ffff72ed840 in __libc_start_main (main=0x5dba40 <main>, argc=0x4, argv=
    fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffffe498) at
#18 0x00000000005dd119 in _start ()
```

```
gdb-peda$ disass $pc-32,$pc+32
Dump of assembler code from 0x38aaf0b to 0x38aaf4b:
   0x00000000038aaf0b <av_freep+27>:    add    BYTE PTR [rax],al
   0x00000000038aaf0d <av_freep+29>:    call   0x38af730 <__afl_maybe_log>
   0x00000000038aaf12 <av_freep+34>:    mov    rax,QWORD PTR [rsp+0x10]
   0x00000000038aaf17 <av_freep+39>:    mov    rcx,QWORD PTR [rsp+0x8]
   0x00000000038aaf1c <av_freep+44>:    mov    rdx,QWORD PTR [rsp]
   0x00000000038aaf20 <av_freep+48>:    lea    rsp,[rsp+0x98]
   0x00000000038aaf28 <av_freep+56>:    mov    rax,rdi
=> 0x00000000038aaf2b <av_freep+59>:    mov    rdi,QWORD PTR [rdi]
   0x00000000038aaf2e <av_freep+62>:    mov    QWORD PTR [rax],0x0
   0x00000000038aaf35 <av_freep+69>:    jmp    0x404140 <free@plt>
   0x00000000038aaf3a:  nop    WORD PTR [rax+rax*1+0x0]
   0x00000000038aaf40 <av_mallocz+0>:   lea    rsp,[rsp-0x98]
   0x00000000038aaf48 <av_mallocz+8>:   mov    QWORD PTR [rsp],rdx
End of assembler dump.
```

```
gdb-peda$ info all-registers
rax            0x433f08b2c82f1376       0x433f08b2c82f1376
rbx            0x433f08b2c82f1356       0x433f08b2c82f1356
rcx            0x7ffff7247040   0x7ffff7247040
rdx            0x3      0x3
rsi            0x0      0x0
rdi            0x433f08b2c82f1376       0x433f08b2c82f1376
rbp            0x10     0x10
rsp            0x7fffffffd318   0x7fffffffd318
r8             0x102e   0x102e
r9             0x0      0x0
r10            0x0      0x0
r11            0x433f08b2c826b8c6       0x433f08b2c826b8c6
r12            0xff     0xff
r13            0x0      0x0
r14            0xd      0xd
r15            0x49bb200        0x49bb200
rip            0x38aaf2b        0x38aaf2b <av_freep+59>
eflags         0x10206  [ PF IF RF ]
cs             0x33     0x33
ss             0x2b     0x2b
ds             0x0      0x0
es             0x0      0x0
fs             0x0      0x0
gs             0x0      0x0
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    0x37f
fstat          0x0      0x0
ftag           0xffff   0xffff
fiseg          0x0      0x0
fioff          0x0      0x0
foseg          0x0      0x0
fooff          0x0      0x0
```

```
fop             0x0     0x0
mxcsr           0x1fa0  [ PE IM DM ZM OM UM PM ]
```

Please confirm.
Thanks

Attachments (1)

- poc(155.5 KB) - added by lys404 2 years ago.

Change History (3)

by lys404, 2 years ago

Attachment: *poc*added

comment:1 by Carl Eugen Hoyos, 2 years ago

Component:	undetermined → avcodec
Keywords:	aac crash SIGSEGV added
Priority:	normal → important
Reproduced by developer:	set
Status:	new → open
Version:	unspecified → git-master

Likely related to ~~#3845~~

comment:2 by Carl Eugen Hoyos, 2 years ago

Resolution:	→ fixed
Status:	open → closed

Fixed by Jan Ekström in d6f293353c94c7ce200f6e0975ae3de49787f91f

Note: See TracTickets for help on using tickets.