

Triggered by ./avconv -y -i POC2

Version:12.3

The output information is as follows:

```
$ ./avconv -y -i POC2
avconv version 12.3, Copyright (c) 2000-2018 the Libav developers
  built on May 11 2018 02:18:02 with gcc 5.4.0 (Ubuntu 5.4.0-6ubuntu1~16.04.9) 20160609
[aac @ 0x4263060] Format detected only with low score of 1, misdetection possible!
[aac @ 0x426ef40] Expected to read 1 SBR bytes actually read 4.
[aac @ 0x426ef40] channel element 1.6 is not allocated
Segmentation fault (core dumped)
```

GDB debugging information is as follows:

```
(gdb) set args -y -i POC2
(gdb) r
```

```
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
avconv version 12.3, Copyright (c) 2000-2018 the Libav developers
  built on May 11 2018 02:18:02 with gcc 5.4.0 (Ubuntu 5.4.0-6ubuntu1~16.04.9) 20160609
[aac @ 0x29b5060] Format detected only with low score of 1, misdetection possible!
[aac @ 0x29c0f40] Expected to read 1 SBR bytes actually read 4.
[aac @ 0x29c0f40] channel element 1.6 is not allocated
```

Program received signal SIGSEGV, Segmentation fault.

```
in_table_int16 (needle=24, last_el=2228256, table=0x7ffffffcf40) at libavcodec/aacsbr.c:171
171         if (table[i] == needle)
```

```
(gdb) bt
```

```
#0  in_table_int16 (needle=24, last_el=2228256, table=0x7ffffffcf40) at libavcodec/aacsbr.c:171
#1  sbr_make_f_tablelim (sbr=sbr@entry=0x7fffff03720) at libavcodec/aacsbr.c:207
#2  0x00000000189d3d0 in sbr_make_f_derived (sbr=0x7fffff03720, ac=0x29c1e60) at
libavcodec/aacsbr.c:605
#3  sbr_reset (sbr=0x7fffff03720, ac=0x29c1e60) at libavcodec/aacsbr.c:1043
#4  ff_decode_sbr_extension (ac=ac@entry=0x29c1e60, sbr=sbr@entry=0x7fffff03720,
  gb_host=gb_host@entry=0x7ffffffd300, crc=crc@entry=0, cnt=cnt@entry=1,
  id_aac=id_aac@entry=1)
  at libavcodec/aacsbr.c:1089
#5  0x00000000187a2cb in decode_extension_payload (elem_type=<optimized out>,
  che=<optimized out>, cnt=1,
  gb=0x7ffffffd300, ac=<optimized out>) at libavcodec/aacdec.c:2240
```

```

#6 aac_decode_frame_int (avctx=avctx@entry=0x29c0f40, data=data@entry=0x29c1be0,
  got_frame_ptr=got_frame_ptr@entry=0x7ffffffd3d4, gb=gb@entry=0x7ffffffd300) at
libavcodec/aacdec.c:2918
#7 0x00000000187fa9b in aac_decode_frame (avctx=0x29c0f40, data=0x29c1be0,
  got_frame_ptr=0x7ffffffd3d4,
  avpkt=<optimized out>) at libavcodec/aacdec.c:3011
#8 0x0000000015164ee in avcodec_decode_audio4 (avctx=avctx@entry=0x29c0f40,
  frame=0x29c1be0,
  got_frame_ptr=got_frame_ptr@entry=0x7ffffffd3d4, avpkt=avpkt@entry=0x7ffffffd470) at
libavcodec/utils.c:1653
#9 0x0000000015172c0 in do_decode (avctx=avctx@entry=0x29c0f40,
  pkt=pkt@entry=0x7ffffffd470)
  at libavcodec/utils.c:1732
#10 0x000000001517e2b in avcodec_send_packet (avctx=avctx@entry=0x29c0f40,
  avpkt=<optimized out>,
  avpkt@entry=0x7ffffffd470) at libavcodec/utils.c:1804
#11 0x0000000009be1dd in try_decode_frame (st=st@entry=0x29c0860,
  avpkt=avpkt@entry=0x7ffffffd560,
  options=<optimized out>, s=0x29b5060) at libavformat/utils.c:1950
#12 0x0000000009d32bf in avformat_find_stream_info (ic=0x29b5060, options=0x29c13c0) at
libavformat/utils.c:2356
#13 0x00000000051f5fe in open_input_file (o=o@entry=0x7ffffffd9d0, filename=<optimized
  out>) at avconv_opt.c:771
#14 0x000000000526ec4 in open_files (l=0x29b5898, l=0x29b5898, open_file=0x51ea90
  <open_input_file>,
  inout=0x1ecc15c "input") at avconv_opt.c:2380
#15 avconv_parse_options (argc=argc@entry=4, argv=argv@entry=0x7ffffffe4c8) at
avconv_opt.c:2417
#16 0x0000000004f015c in main (argc=4, argv=0x7ffffffe4c8) at avconv.c:2883
(gdb) l

```

```

166
167 static inline int in_table_int16(const int16_t *table, int last_el, int16_t needle)
168 {
169     int i;
170     for (i = 0; i <= last_el; i++)
171         if (table[i] == needle)
172             return 1;
173     return 0;
174 }
175
(gdb)

```

```

(gdb) info all-registers

```

rax	0x7fffffff000	140737488351232
rbx	0x7ffff7f03720	140737353103136
rcx	0x16	22
rdx	0x18	24
rsi	0x1060	4192
rdi	0x7ffff7f43b42	140737353366338
rbp	0x7ffff7f43b32	0x7ffff7f43b32
rsp	0x7ffffffcf30	0x7ffffffcf30
r8	0x7ffff7f43b58	140737353366360
r9	0x220020	2228256
r10	0x22002e	2228270
r11	0x22002e	2228270
r12	0xb 11	
r13	0x1059	4185
r14	0x5 5	
r15	0x3a	58
rip	0x188e31f	0x188e31f <sbr_make_f_tablelim+3359>
eflags	0x10216	[PF AF IF RF]
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)