

Triggered by ./avconv -y -i POC

Version:12.3

The output information is as follows:

```
$ ./avconv -y -i POC
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
Segmentation fault (core dumped)
```

GDB debugging information is as follows:

```
(gdb) set args -y -i POC
(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
```

Program received signal SIGSEGV, Segmentation fault.

```
mov_probe (p=p@entry=0x7ffffffd660) at libavformat/mov.c:3340
3340      switch(tag) {
(gdb) bt
#0  mov_probe (p=p@entry=0x7ffffffd660) at libavformat/mov.c:3340
#1  0x000000000069e4d0 in av_probe_input_format2 (is_opened=1, score_max=<synthetic
pointer>,
    pd=0x7ffffffd640) at libavformat/format.c:193
#2  av_probe_input_buffer (pb=0x29c8980, fmt=0x29b5068,
    filename=filename@entry=0x7ffffffe73a "POC",
    logctx=logctx@entry=0x29b5060, offset=offset@entry=0, max_probe_size=1048576) at
libavformat/format.c:286
#3  0x00000000009e34fd in init_input (options=0x7ffffffd710, filename=0x7ffffffe73a "POC",
    s=0x29b5060)
    at libavformat/utils.c:214
#4  avformat_open_input (ps=ps@entry=0x7ffffffd7d0, filename=filename@entry=0x7ffffffe73a
"POC",
    fmt=fmt@entry=0x0, options=0x29baff8) at libavformat/utils.c:303
#5  0x000000000051f1e2 in open_input_file (o=o@entry=0x7ffffffd9d0, filename=<optimized
out>)
    at avconv_opt.c:754
```

#6 0x0000000000526ec4 in open_files (l=0x29b5898, l=0x29b5898, open_file=0x51ea90
<open_input_file>,
inout=0x1ecc15c "input") at avconv_opt.c:2380
#7 avconv_parse_options (argc=argc@entry=4, argv=argv@entry=0x7ffffffe4c8) at
avconv_opt.c:2417
#8 0x00000000004f015c in main (argc=4, argv=0x7ffffffe4c8) at avconv.c:2883

(gdb) l

```
3335     for (;;) {
3336         /* ignore invalid offset */
3337         if ((offset + 8) > (unsigned int)p->buf_size)
3338             return score;
3339         tag = AV_RL32(p->buf + offset + 4);
3340         switch(tag) {
3341             /* check for obvious tags */
3342             case MKTAG('J','P',' ',' '): /* jpeg 2000 signature */
3343             case MKTAG('m','o','o','v'):
3344             case MKTAG('m','d','a','t'):
```

(gdb) info all-registers

rax	0x32	50
rbx	0x1ec3fe4	32260068
rcx	0xffffffff	4294967295
rdx	0x64697575	1684632949
rsi	0xffffffff	4294967295
rdi	0x29c8a40	43813440
rbp	0x0 0x0	
rsp	0x7ffffffd5f8	0x7ffffffd5f8
r8	0xd 13	
r9	0x7 7	
r10	0x0 0	
r11	0x29c8a4d	43813453
r12	0x800	2048
r13	0x73ef50	7597904
r14	0x2392c00	37301248
r15	0x7ffffffd680	140737488344704
rip	0x73f012	0x73f012 <mov_probe+194>
eflags	0x10297	[CF PF AF SF 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)