New issue

Jump to bottom

SEGV sao.cc: in void apply_sao_internal<unsigned short> #352

Open FDU-Sec opened this issue on Oct 10 · 0 comments

FDU-Sec commented on Oct 10

Description

SEGV /libde265/libde265/sao.cc:231 in void apply_sao_internal(de265_image*, int, int, slice_segment_header const*, int, int, int, unsigned short const*, int, unsigned short*, int)

Version

```
$ ./dec265 -h
 dec265  v1.0.8
--------------
usage: dec265 [options] videofile.bin
The video file must be a raw bitstream, or a stream with NAL units (option -n).

options:
  -q, --quiet       do not show decoded image
  -t, --threads N   set number of worker threads (0 - no threading)
  -c, --check-hash  perform hash check
  -n, --nal         input is a stream with 4-byte length prefixed NAL units
  -f, --frames N    set number of frames to process
  -o, --output      write YUV reconstruction
  -d, --dump        dump headers
  -0, --noaccel     do not use any accelerated code (SSE)
  -v, --verbose     increase verbosity level (up to 3 times)
  -L, --no-logging  disable logging
  -B, --write-bytestream FILENAME  write raw bytestream (from NAL input)
  -m, --measure YUV compute PSNRs relative to reference YUV
  -T, --highest-TID select highest temporal sublayer to decode
      --disable-deblocking   disable deblocking filter
      --disable-sao          disable sample-adaptive offset filter
  -h, --help        show help
```

Replay

```
git clone https://github.com/strukturag/libde265.git
cd libde265
mkdir build
cd build
cmake ../ -DCMAKE_CXX_FLAGS="-fsanitize=address"
make -j$(nproc)
./dec265/dec265 poc18
```

ASAN

```
WARNING: non-existing PPS referenced
WARNING: non-existing PPS referenced
WARNING: slice header invalid
WARNING: slice header invalid
WARNING: slice header invalid
ASAN:DEADLYSIGNAL
=================================================================
==24487==ERROR: AddressSanitizer: SEGV on unknown address 0x61106a5b8d93 (pc 0x55dd23192a5c bp 0x0c2c
==24487==The signal is caused by a READ memory access.
    #0 0x55dd23192a5b in void apply_sao_internal<unsigned short>(de265_image*, int, int, slice_segmen
    #1 0x55dd2318b477 in void apply_sao<unsigned char>(de265_image*, int, int, slice_segment_header c
    #2 0x55dd2318b477 in apply_sample_adaptive_offset_sequential(de265_image*) /libde265/libde265/sao
    #3 0x55dd230bd468 in decoder_context::run_postprocessing_filters_sequential(de265_image*) /libde2
    #4 0x55dd230bd468 in decoder_context::decode_some(bool*) /libde265/libde265/decctx.cc:778
    #5 0x55dd230ce78b in decoder_context::read_slice_NAL(bitreader&, NAL_unit*, nal_header&) /libde26
    #6 0x55dd230d0729 in decoder_context::decode_NAL(NAL_unit*) /libde265/libde265/decctx.cc:1239
    #7 0x55dd230d15a9 in decoder_context::decode(int*) /libde265/libde265/decctx.cc:1327
    #8 0x55dd23088be5 in main /libde265/dec265/dec265.cc:764
    #9 0x7fed8173ac86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #10 0x55dd2308b0f9 in _start (/libde265/dec265/dec265+0x1b0f9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /libde265/libde265/sao.cc:231 in void apply_sao_internal<unsigned sho
==24487==ABORTING
```

POC

https://github.com/FDU-Sec/poc/blob/main/libde265/poc18

Environment

```
Ubuntu 18.04.5 LTS
Clang 10.0.1
gcc 7.5.0
```

Credit

Peng Deng (Fudan University)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant