New issue

Jump to bottom

segment fault in apply_sao_internal when decoding file #234

Open leonzhao7 opened this issue on Dec 24, 2019 · 1 comment

leonzhao7 commented on Dec 24, 2019

segment fault in apply_sao_internal when decoding file

I found some problems during fuzzing

Test Version

dev version, git clone https://github.com/strukturag/libde265

Test Environment

root@ubuntu:~# lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description: Ubuntu 16.04.6 LTS
Release: 16.04
Codename: xenial

root@ubuntu:~# uname -a
Linux ubuntu 4.15.0-45-generic #4816.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux

Test Configure

./configure
configure: --
configure: Building dec265 example: yes
configure: Building sherlock265 example: no
configure: Building encoder: yes
configure: --

Test Program

```
dec265 [infile]
```

Asan Output

```
root@ubuntu:~# ./dec265 libde265-apply_sao_internal-segment.crash
WARNING: non-existing PPS referenced
WARNING: non-existing PPS referenced
WARNING: end_of_sub_stream_one_bit not set to 1 when it should be
WARNING: end_of_sub_stream_one_bit not set to 1 when it should be
WARNING: pps header invalid
ASAN:SIGSEGV
=================================================================
==34516==ERROR: AddressSanitizer: SEGV on unknown address 0x62c02b4f5c83 (pc 0x00000045b20d bp 0x7ffc86181280 sp 0x7ffc86180f90 T0)
    #0 0x45b20c in void apply_sao_internal<unsigned short>(de265_image*, int, int, slice_segment_header const*, int, int, int, unsigned short const*, int, unsigned short*, int)
/root/src/libde265/libde265/sao.cc:252
    #1 0x45973e in void apply_sao<unsigned char>(de265_image*, int, int, slice_segment_header const*, int, int, int, unsigned char const*, int, unsigned char*, int)
/root/src/libde265/libde265/sao.cc:270
    #2 0x457778 in apply_sample_adaptive_offset_sequential(de265_image*) /root/src/libde265/libde265/sao.cc:361
    #3 0x413beb in decoder_context::run_postprocessing_filters_sequential(de265_image*) /root/src/libde265/libde265/decctx.cc:1889
    #4 0x40b849 in decoder_context::decode_some(bool*) /root/src/libde265/libde265/decctx.cc:769
    #5 0x40e23e in decoder_context::decode(int*) /root/src/libde265/libde265/decctx.cc:1329
    #6 0x405a61 in de265_decode /root/src/libde265/libde265/de265.cc:346
    #7 0x404972 in main /root/src/libde265/dec265/dec265.cc:764
    #8 0x7f71b014282f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #9 0x402b28 in _start (/root/dec265+0x402b28)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /root/src/libde265/libde265/sao.cc:252 void apply_sao_internal<unsigned short>(de265_image*, int, int, slice_segment_header const*, int, int, int,
unsigned short const*, int, unsigned short*, int)
==34516==ABORTING
```

POC file

libde265-apply_sao_internal-segment.zip
password: leon.zhao.7

CREDIT

Zhao Liang, Huawei Weiran Labs

coldtobi commented last week

According to Debian this is CVE-2020-21605

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants