New issue

Jump to bottom

# Segmentation fault in refinementscan.cpp:644 #42

Closed seviezhou opened this issue on Aug 13, 2020 · 1 comment

seviezhou commented on Aug 13, 2020

## System info

Ubuntu x86_64, gcc (Ubuntu 5.5.0-12ubuntu1), jpeg (latest master e52406)

## Command line

./jpeg -oz -h -s 1x1,2x2,2x2 @@ /dev/null

## AddressSanitizer output

```
ASAN:SIGSEGV
=================================================================
==12664==ERROR: AddressSanitizer: SEGV on unknown address 0x0000000001d2 (pc 0x0000004a33fc bp 0x7ffed315df90 sp 0x7ffed315df70 T0)
    #0 0x4a33fb in HuffmanDecoder::Get(BitStream<false>*) ../coding/huffmandecoder.hpp:112
    #1 0x4fdeaa in RefinementScan::DecodeBlock(int*, HuffmanDecoder*, unsigned short&) /home/seviezhou/libjpeg/codestream/refinementscan.cpp:644
    #2 0x4ff7fc in RefinementScan::ParseMCU() /home/seviezhou/libjpeg/codestream/refinementscan.cpp:314
    #3 0x45c4b4 in JPEG::ReadInternal(JPG_TagItem*) /home/seviezhou/libjpeg/interface/jpeg.cpp:345
    #4 0x45d5be in JPEG::Read(JPG_TagItem*) /home/seviezhou/libjpeg/interface/jpeg.cpp:210
    #5 0x42adbf in Reconstruct(char const*, char const*, int, char const*, bool) /home/seviezhou/libjpeg/cmd/reconstruct.cpp:121
    #6 0x4055f0 in main /home/seviezhou/libjpeg/cmd/main.cpp:718
    #7 0x7fd6ee82983f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #8 0x409da8 in _start (/home/seviezhou/libjpeg/jpeg+0x409da8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ../coding/huffmandecoder.hpp:112 HuffmanDecoder::Get(BitStream<false>*)
==12664==ABORTING
```

## POC

SEGV-DecodeBlock-refinementscan-644.zip

thorfdbg commented on Aug 28, 2020 Owner

Thanks, found & fixed.

thorfdbg closed this as completed on Aug 28, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants