New issue

Jump to bottom

Segmentation fault in sampleinterleavedlsscan.cpp:133 #37

Closed seviezhou opened this issue on Aug 4, 2020 · 3 comments

seviezhou commented on Aug 4, 2020

System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), jpeg (latest master e52406)

Command line

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

Output

```
Segmentation fault
```

AddressSanitizer output

```
ASAN:SIGSEGV
=================================================================
==81357==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x0000005200b8 bp 0x7ffdd2f954b0 sp 0x7ffdd2f95110 T0)
    #0 0x5200b7 in SampleInterleavedLSScan::ParseMCU() /home/seviezhou/libjpeg/codestream/sampleinterleavedlsscan.cpp:133
    #1 0x45c4b4 in JPEG::ReadInternal(JPG_TagItem*) /home/seviezhou/libjpeg/interface/jpeg.cpp:345
    #2 0x45d5be in JPEG::Read(JPG_TagItem*) /home/seviezhou/libjpeg/interface/jpeg.cpp:210
    #3 0x42adbf in Reconstruct(char const*, char const*, int, char const*, bool) /home/seviezhou/libjpeg/cmd/reconstruct.cpp:121
    #4 0x4055f0 in main /home/seviezhou/libjpeg/cmd/main.cpp:718
    #5 0x7ff8b3e8083f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #6 0x409da8 in _start (/home/seviezhou/libjpeg/jpeg+0x409da8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/seviezhou/libjpeg/codestream/sampleinterleavedlsscan.cpp:133 SampleInterleavedLSScan::ParseMCU()
==81357==ABORTING
```

POC

SEGV-ParseMCU-sampleinterleavedlsscan-133.zip

thorfdbg commented on Aug 29, 2020 Owner

Caused by pulling in the same component twice in the SOS marker. Fixed. Thank you.

thorfdbg closed this as completed on Aug 29, 2020

attritionorg commented on Sep 24, 2020 Contributor

@thorfdbg I am trying to find where you fixed this and based on commits, it wasn't done in sampleinterleavedlsscan.cpp. Can you point to the fixing commit / where you implemented? Thanks!

thorfdbg commented on Sep 25, 2020 Owner

If this is about having two identical components in a scan, this issue was addressed in scan.cpp, lines 147 to 150.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants