New issue

Jump to bottom

Segmentation fault in blockbitmaprequester.cpp:1047 #33

Closed **seviezhou** opened this issue on Aug 3, 2020 · 1 comment

seviezhou commented on Aug 3, 2020 • edited

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

```
*** Warning -1038 in Tables::ParseTables, line 1384, file tables.cpp
*** Reason is: found invalid marker, probably a marker size is out of range

*** Warning -1038 in Frame::StartParseHiddenScan, line 869, file frame.cpp
*** Reason is: Start of Scan SOS marker missing

*** Warning -1038 in Frame::ParseTrailer, line 1083, file frame.cpp
*** Reason is: missing an EOI marker at the end of the stream

*** Warning -1038 in Image::ParseTrailer, line 1464, file image.cpp
*** Reason is: expecting an EOI marker at the end of the stream

Segmentation fault
```

AddressSanitizer output

```
ASAN:SIGSEGV
=================================================================
==56860==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x00000086f67b bp 0x7ffcf2756d80 sp 0x7ffcf2756c20 T0)
    #0 0x86f67a in BlockBitmapRequester::ReconstructUnsampled(RectangleRequest const*, RectAngle<int> const&, unsigned int, ColorTrafo*)
/home/seviezhou/libjpeg/control/blockbitmaprequester.cpp:1047
    #1 0x486b6c in Image::ReconstructRegion(BitMapHook*, RectangleRequest const*) /home/seviezhou/libjpeg/codestream/image.cpp:1111
    #2 0x45f10a in JPEG::InternalDisplayRectangle(JPG_TagItem*) /home/seviezhou/libjpeg/interface/jpeg.cpp:721
    #3 0x45f452 in JPEG::DisplayRectangle(JPG_TagItem*) /home/seviezhou/libjpeg/interface/jpeg.cpp:699
    #4 0x42c573 in Reconstruct(char const*, char const*, int, char const*, bool) /home/seviezhou/libjpeg/cmd/reconstruct.cpp:320
    #5 0x4055f0 in main /home/seviezhou/libjpeg/cmd/main.cpp:718
    #6 0x7fe0a1fc283f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #7 0x409da8 in _start (/home/seviezhou/libjpeg/jpeg+0x409da8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/seviezhou/libjpeg/control/blockbitmaprequester.cpp:1047 BlockBitmapRequester::ReconstructUnsampled(RectangleRequest const*, RectAngle<int>
const&, unsigned int, ColorTrafo*)
==56860==ABORTING
```

POC

SEGV-ReconstructUnsampled-blockbitmaprequester-1047.zip

seviezhou changed the title ~~Segmentation fault in entropyparser.cpp:134~~ Segmentation fault in blockbitmaprequester.cpp:1047 on Aug 3, 2020

thorfdbg commented on Aug 29, 2020 Owner

Caused by never starting a scan, then attempting to decode an image. Fixed, thank you.

thorfdbg closed this as completed on Aug 29, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants