New issue

Jump to bottom

Segmentation fault in blockbitmaprequester.cpp:1182 #34

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

seviezhou commented on Aug 3, 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

```
*** Warning -1038 in Frame::ParseTrailer, line 1088, file frame.cpp
*** Reason is: expecting a marker or marker segment - stream is out of sync

Segmentation fault
```

AddressSanitizer output

```
ASAN:SIGSEGV
=================================================================
==26800==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x000000873314 bp 0x7ffe658218c0 sp 0x7ffe65821780 T0)
    #0 0x873313 in BlockBitmapRequester::PushReconstructedData(RectangleRequest const*, RectAngle<int> const&, unsigned int, ColorTrafo*)
/home/seviezhou/libjpeg/control/blockbitmaprequester.cpp:1182
    #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 0x7fdecbdba83f 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:1182 BlockBitmapRequester::PushReconstructedData(RectangleRequest const*, RectAngle<int>
const&, unsigned int, ColorTrafo*)
==26800==ABORTING
```

POC

SEGV-PushReconstructedData-blockbitmaprequester-1182.zip

thorfdbg commented on Aug 29, 2020 Owner

Fixed as part of another bug, component pulled in twice. 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