<> Code   ⊙ Issues 2   ⊓ Pull requests 7   ⊙ Actions   ⊞ Projects   ⊞ Wiki   ...

New issue   Jump to bottom

Segmentation fault in blockbitmaprequester.cpp:1100 #28

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

---

seviezhou commented on Aug 1, 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

```
For license conditions, see README.license for details.

*** 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

```
=================================================================
==15013==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x00000087109c bp 0x7fff76b3e9c0 sp 0x7fff76b3e760 T0)
    #0 0x87109b in BlockBitmapRequester::PullQData(RectangleRequest const*, RectAngle<int> const&) /home/seviezhou/libjpeg/control/blockbitmaprequester.cpp:1100
    #1 0x8742e9 in BlockBitmapRequester::ReconstructRegion(RectAngle<int> const&, RectangleRequest const*) /home/seviezhou/libjpeg/control/blockbitmaprequester.cpp:1249
    #2 0x486b6c in Image::ReconstructRegion(BitMapHook*, RectangleRequest const*) /home/seviezhou/libjpeg/codestream/image.cpp:1111
    #3 0x45f10a in JPEG::InternalDisplayRectangle(JPG_TagItem*) /home/seviezhou/libjpeg/interface/jpeg.cpp:721
    #4 0x45f452 in JPEG::DisplayRectangle(JPG_TagItem*) /home/seviezhou/libjpeg/interface/jpeg.cpp:699
    #5 0x42c573 in Reconstruct(char const*, char const*, int, char const*, bool) /home/seviezhou/libjpeg/cmd/reconstruct.cpp:320
    #6 0x4055f0 in main /home/seviezhou/libjpeg/cmd/main.cpp:718
    #7 0x7f727943883f 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 /home/seviezhou/libjpeg/control/blockbitmaprequester.cpp:1100 BlockBitmapRequester::PullQData(RectangleRequest const*, RectAngle<int> const&)
==15013==ABORTING
```

POC

SEGV-PullQData-blockbitmaprequester-1100.zip

✏️ 🟢 **seviezhou** changed the title ~~Segmentation fault in image.cpp:1464~~ Segmentation fault in blockbitmaprequester.cpp:1100 on Aug 3, 2020

---

thorfdbg commented on Aug 29, 2020   Owner

No longer reproducible, probably closed as part of another bug. Re-open if it reappears.

🟢 **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