

[New issue](#)[Jump to bottom](#)

Segmentation fault in LineMerger::GetNextLowpassLine #79

✓ Closed chluo911 opened this issue on Jul 28 · 3 comments

chluo911 commented on Jul 28 • edited ▼

Hi, there.

There is a segmentation fault in the newest master branch.

Here is the reproducing command:

```
jpeg poc /dev/null
```

```
(gdb) bt
```

```
#0 0x00007ffff7f31270 in ?? () from /lib/x86_64-linux-gnu/libc.so.6
#1 0x0000000000711b6f in LineMerger::GetNextLowpassLine (this=0x85ed20, comp=2 '\002')
    at linemerger.cpp:262
#2 0x00000000007127d2 in LineMerger::GetNextExpandedLowPassLine (this=0x85ed20,
    comp=<optimized out>) at linemerger.cpp:339
#3 0x0000000000713251 in LineMerger::GetNextLine (this=0x85ed20, comp=2 '\002')
    at linemerger.cpp:360
#4 0x000000000071c2dd in HierarchicalBitmapRequester::Pull8Lines (this=0x792720,
    c=<optimized out>) at hierarchicalbitmaprequester.cpp:447
#5 0x0000000000720156 in HierarchicalBitmapRequester::ReconstructRegion (this=0x792720,
    orgregion=..., rr=0x7fffffffdae8) at hierarchicalbitmaprequester.cpp:739
#6 0x000000000045c501 in Image::ReconstructRegion (this=0x7923b0, bmh=0x7fffffff790,
    rr=0x7fffffffdae8) at image.cpp:1115
#7 0x000000000043e266 in JPEG::InternalDisplayRectangle (this=0x7904c8, tags=0x7fffffffde90)
    at jpeg.cpp:721
#8 0x000000000043e14b in JPEG::DisplayRectangle (this=0x7904c8, tags=0x7fffffffde90)
    at jpeg.cpp:699
#9 0x000000000041e336 in Reconstruct (infile=<optimized out>,
    outfile=0x7fffffff704 "/dev/null", colortrafo=1,
    alpha=0x790280 "\230$\255", <incomplete sequence \373>, upsample=true)
    at reconstruct.cpp:331
#10 0x0000000000408b6a in main (argc=<optimized out>, argv=0x87a720) at main.cpp:747
```

[poc.zip](#)

thorfdbg commented on Aug 3

Owner

Unfortunately, I cannot reproduce this issue.

chluo911 commented on Aug 3 • edited ▼

Author


Sorry, I found I attached the wrong file. I just updated the attached PoC file. Please check that.

thorfdbg commented on Aug 3

Owner

Thank you, this should be fixed in the latest trunk.



 thorfdbg closed this as completed on Aug 3

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

