New issue

Jump to bottom

Segmentation fault in HuffmanDecoder::Get #78

Closed chluo911 opened this issue on Jul 27 · 1 comment

chluo911 commented on Jul 27

Hi, there.

There is a segmentation fault in the newest master branch.

Here is the reproducing command:

```
jpeg poc /dev/null


  Program received signal SIGSEGV, Segmentation fault.
  HuffmanDecoder::Get (this=0x0, io=0x7933c8)
      at /home/users/chluo/libjpeg/codestream/../coding/huffmandecoder.hpp:112
  warning: Source file is more recent than executable.
  (gdb) bt
  #0  HuffmanDecoder::Get (this=0x0, io=0x7933c8)
      at /home/users/chluo/libjpeg/codestream/../coding/huffmandecoder.hpp:112
  #1  0x0000000000491388 in LosslessScan::ParseMCU (this=0x793250, prev=0x7fffffffda90,
      top=0x7fffffffda70) at losslessscan.cpp:374
  #2  0x0000000000491b4a in LosslessScan::ParseMCU (this=0x793250)
      at losslessscan.cpp:440
  #3  0x000000000043aca1 in JPEG::ReadInternal (this=0x7904c8, tags=0x7fffffffdd40)
      at jpeg.cpp:345
  #4  0x000000000043988b in JPEG::Read (this=0x7904c8, tags=0x7fffffffdd40)
      at jpeg.cpp:210
  #5  0x000000000041cabb in Reconstruct (infile=<optimized out>,
      outfile=0x7fffffffe6fc "/dev/null", colortrafo=1, alpha=0x0, upsample=true)
      at reconstruct.cpp:121
  #6  0x0000000000408b6a in main (argc=<optimized out>, argv=0x0) at main.cpp:747
```

poc.zip

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