New issue

Jump to bottom

# A heap overflow in linebuffer.cpp:322 causes segment fault #35

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

*** 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

```
=================================================================
==35214==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x611000009fd0 at pc 0x7f06d39ea935 bp 0x7fff3a80bdc0 sp 0x7fff3a80b568
READ of size 32 at 0x611000009fd0 thread T0
    #0 0x7f06d39ea934 in __asan_memcpy (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x8c934)
    #1 0x8583e2 in LineBuffer::FetchRegion(int, Line const*, int*) /home/seviezhou/libjpeg/control/linebuffer.cpp:322
    #2 0x87ef78 in LineBitmapRequester::ReconstructRegion(RectAngle<int> const&, RectangleRequest const*) /home/seviezhou/libjpeg/control/linebitmaprequester.cpp:513
    #3 0x486b6c in Image::ReconstructRegion(BitMapHook*, RectangleRequest const*) /home/seviezhou/libjpeg/codestream/image.cpp:1111
    #4 0x45f10a in JPEG::InternalDisplayRectangle(JPG_TagItem*) /home/seviezhou/libjpeg/interface/jpeg.cpp:721
    #5 0x45f452 in JPEG::DisplayRectangle(JPG_TagItem*) /home/seviezhou/libjpeg/interface/jpeg.cpp:699
    #6 0x42c573 in Reconstruct(char const*, char const*, int, char const*, bool) /home/seviezhou/libjpeg/cmd/reconstruct.cpp:320
    #7 0x4055f0 in main /home/seviezhou/libjpeg/cmd/main.cpp:718
    #8 0x7f06d2ec883f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #9 0x409da8 in _start (/home/seviezhou/libjpeg/jpeg+0x409da8)

0x611000009fd0 is located 0 bytes to the right of 208-byte region [0x611000009f00,0x611000009fd0)
allocated by thread T0 here:
    #0 0x7f06d39f6602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
    #1 0x44cadf in Environ::CoreAllocMem(unsigned int, unsigned int) /home/seviezhou/libjpeg/tools/environment.cpp:664
    #2 0x856107 in LineBuffer::StartMCUQuantizerRow(Scan*) /home/seviezhou/libjpeg/control/linebuffer.cpp:227
    #3 0x45c94d in JPEG::ReadInternal(JPG_TagItem*) /home/seviezhou/libjpeg/interface/jpeg.cpp:324
    #4 0x45d5be in JPEG::Read(JPG_TagItem*) /home/seviezhou/libjpeg/interface/jpeg.cpp:210
    #5 0x42adbf in Reconstruct(char const*, char const*, int, char const*, bool) /home/seviezhou/libjpeg/cmd/reconstruct.cpp:121
    #6 0x4055f0 in main /home/seviezhou/libjpeg/cmd/main.cpp:718
    #7 0x7f06d2ec883f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)

SUMMARY: AddressSanitizer: heap-buffer-overflow ??:0 __asan_memcpy
Shadow bytes around the buggy address:
  0x0c227fff93a0: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa fa fa
  0x0c227fff93b0: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c227fff93c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c227fff93d0: 00 00 fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff93e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c227fff93f0: 00 00 00 00 00 00 00 00 00 00 00[fa]fa fa fa fa
  0x0c227fff9400: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff9410: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff9420: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff9430: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff9440: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
==35214==ABORTING
```

## POC

heap-overflow-FetchRegion-linebuffer-322.zip

**thorfdbg** commented on Aug 29, 2020 Owner

Fixed as part of another bug, no longer applies. 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