New issue

Jump to bottom

A heap overflow in aclosslessscan.cpp:349 causes segment fault #36

Closed seviezhou opened this issue on Aug 3, 2020 · 2 comments

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 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

```
=================================================================
==74952==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61a00001f774 at pc 0x0000004f2c69 bp 0x7ffcf95a51b0 sp 0x7ffcf95a51a0
READ of size 4 at 0x61a00001f774 thread T0
    #0 0x4f2c68 in ACLosslessScan::ParseMCU(Line**, Line**) /home/seviezhou/libjpeg/codestream/aclosslessscan.cpp:349
    #1 0x4f3385 in ACLosslessScan::ParseMCU() /home/seviezhou/libjpeg/codestream/aclosslessscan.cpp:471
    #2 0x45c4b4 in JPEG::ReadInternal(JPG_TagItem*) /home/seviezhou/libjpeg/interface/jpeg.cpp:345
    #3 0x45d5be in JPEG::Read(JPG_TagItem*) /home/seviezhou/libjpeg/interface/jpeg.cpp:210
    #4 0x42adbf in Reconstruct(char const*, char const*, int, char const*, bool) /home/seviezhou/libjpeg/cmd/reconstruct.cpp:121
    #5 0x4055f0 in main /home/seviezhou/libjpeg/cmd/main.cpp:718
    #6 0x7f2ee6e9783f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #7 0x409da8 in _start (/home/seviezhou/libjpeg/jpeg+0x409da8)

0x61a00001f774 is located 0 bytes to the right of 1268-byte region [0x61a00001f280,0x61a00001f774)
allocated by thread T0 here:
    #0 0x7f2ee79c5602 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 0x4ef428 in ACLosslessScan::FindComponentDimensions() /home/seviezhou/libjpeg/codestream/aclosslessscan.cpp:130
    #3 0x4ef63c in ACLosslessScan::StartParseScan(ByteStream*, Checksum*, BufferCtrl*) /home/seviezhou/libjpeg/codestream/aclosslessscan.cpp:143
    #4 0x533499 in Frame::StartParseScan(ByteStream*, Checksum*) /home/seviezhou/libjpeg/marker/frame.cpp:847
    #5 0x45bec4 in JPEG::ReadInternal(JPG_TagItem*) /home/seviezhou/libjpeg/interface/jpeg.cpp:296
    #6 0x45d5be in JPEG::Read(JPG_TagItem*) /home/seviezhou/libjpeg/interface/jpeg.cpp:210
    #7 0x42adbf in Reconstruct(char const*, char const*, int, char const*, bool) /home/seviezhou/libjpeg/cmd/reconstruct.cpp:121
    #8 0x4055f0 in main /home/seviezhou/libjpeg/cmd/main.cpp:718
    #9 0x7f2ee6e9783f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/libjpeg/codestream/aclosslessscan.cpp:349 ACLosslessScan::ParseMCU(Line**, Line**)
Shadow bytes around the buggy address:
  0x0c347fffbe90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fffbea0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fffbeb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fffbec0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fffbed0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c347fffbee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00[04]fa
  0x0c347fffbef0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fffbf00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fffbf10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fffbf20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fffbf30: 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
==74952==ABORTING
```

POC

heap-overflow-ParseMCU-aclosslessscan-349.zip

thorfdbg commented on Aug 29, 2020 Owner

No longer applies, closed as part of another bug, and fixed there.

thorfdbg closed this as completed on Aug 29, 2020

xteema commented on Oct 8, 2021

Is this fixed by the commit https://github.com/thorfdbg/libjpeg/commit/97e99771b71ad295cd9aa6ef5f221e002b9b0574

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants