Closed Issue created 5 months ago by 4ugustus

tiffcrop: FPE in computeOutputPixelOffsets, tiffcrop.c:5936 (Different from #347)

Summary

There is a FPE error in computeOutputPixelOffsets, tools/tiffcrop.c:5936. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted tiff file. This is different from #347.

Version

-R 90 -H 300 -O landscape -P 300.0x300.0 -i

Steps to reproduce

```
# CFLAGS="-g -O0" CXXFLAGS="-g -O0" ./configure --prefix=$PWD/build_orig --disable-shared

# make -j; make install; make clean

# ./build_orig/bin/tiffcrop -R 270 -P 300.0x300.0 poc /tmp/foo
TIFFReadDirectoryCheckOrder: Warning, Invalid TIFF directory; tags are not sorted in ascending order
TIFFReadDirectory: Warning, Unknown field with tag 2 (0x2) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 12544 (0x3100) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 65427 (0xff93) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 32768 (0x8000) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 245 (0xf5) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 65407 (0xff7f) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 26003 (0x6593) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 1 (0x1) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 51657 (0xc9c9) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 8393 (0x20c9) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 60361 (0xebc9) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 0 (0x0) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 59136 (0xe700) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 16448 (0x4040) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 25888 (0x6520) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 1024 (0x400) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 65408 (0xff80) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 42 (0x2a) encountered.
TIFFReadDirectory: Warning, Invalid data type for tag StripOffsets.
TIFFFetchNormalTag: Warning, IO error during reading of "Tag 42"; tag ignored.
TIFFReadDirectory: Warning, TIFF directory is missing required "StripByteCounts" field, calculating
TIFFAdvanceDirectory: Error fetching directory count.
loadImage: Image lacks Photometric interpretation tag.
Floating point exception (core dumped)

(gdb) # bt
#0  0x000000000041181a in computeOutputPixelOffsets (crop=0x7fffffff8eb0, image=0x7fffffff8c30,
    page=0x7fffffff8c50, sections=0x7fffffff91a0, dump=0x7fffffffb530) at tiffcrop.c:5936
#1  0x00000000004076d7 in main (argc=0x7, argv=0x7fffffffe688) at tiffcrop.c:2459
#2  0x00007ffff6749840 in __libc_start_main (main=0x406c6d <main>, argc=0x7, argv=0x7fffffffe688,
    init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffffe678)
    at ../csu/libc-start.c:291
#3  0x0000000000402f69 in _start ()
```

Platform

```
# uname -a
Linux 4a409ce47130 5.4.0-70-generic #78~18.04.1-Ubuntu SMP Sat Mar 20 14:10:07 UTC 2021 x86_64 x86_6
```

poc

Edited 5 months ago by 4ugustus

Drag your designs here or click to upload.

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Link issues together to show that they're related or that one is blocking others. Learn more.

Related merge requests 1

fix the FPE in tiffcrop (#415, #427, and #428)
!346

When this merge request is accepted, this issue will be closed automatically.

Activity

4ugustus changed the description 5 months ago ·

4ugustus mentioned in merge request !346 (merged) 5 months ago

4ugustus mentioned in commit `dd1bcc7a` 5 months ago

Even Rouault mentioned in commit `f3a5e010` 5 months ago

Even Rouault closed via merge request !346 (merged) 5 months ago

Please register or sign in to reply