

tiffcrop: FPE in computeOutputPixelOffsets, tiffcrop.c:5802

Summary

There is a FPE in computeOutputPixelOffsets in tools/tiffcrop.c:5802. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted tiff file. **Note that this crash is different from #347.**

Version

LIBTIFF, Version 4.3.0, commit id [5e180045](#) (Fri Feb 25 10:38:31 2022 +0000)

Steps to reproduce

```
# CFLAGS="-g -fsanitize=address -fno-omit-frame-pointer" CXXFLAGS="-g -fsanitize=address -fno-omit-f

# make -j; make install; make clean


./build_asan/bin/tiffcrop -H 341 poc /tmp/foo
TIFFReadDirectoryCheckOrder: Warning, Invalid TIFF directory; tags are not sorted in ascending order
TIFFReadDirectory: Warning, Unknown field with tag 32582 (0x7f46) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 8192 (0x2000) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 304 (0x130) encountered.
poc_tiffcrop/00008: Warning, Nonstandard tile length 65290, convert file.
TIFFReadDirectory: Warning, Unknown field with tag 8232 (0x2028) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 9 (0x9) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 1 (0x1) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 59395 (0xe803) encountered.
TIFFFetchNormalTag: Warning, Incorrect count for "NumberOfInks"; tag ignored.
TIFFFetchNormalTag: Warning, Sanity check on size of "Tag 32582" value failed; tag ignored.
TIFFFetchNormalTag: Warning, IO error during reading of "Tag 8192"; tag ignored.
TIFFReadDirectory: Warning, Invalid data type for tag StripOffsets.
TIFFFetchNormalTag: Warning, Incorrect count for "Orientation"; tag ignored.
TIFFFetchNormalTag: Warning, IO error during reading of "Tag 304"; tag ignored.
TIFFReadDirectory: Warning, Invalid data type for tag StripByteCounts.
TIFFAdvanceDirectory: Error fetching directory count.
loadImage: Image lacks Photometric interpretation tag.
Fax4Decode: Bad code word at line 0 of tile 0 (x 0).
Fax4Decode: Warning, Premature EOL at line 0 of tile 0 (got 0, expected 127).
ASAN:DEADLYSIGNAL
=====
==390948==ERROR: AddressSanitizer: FPE on unknown address 0x5558d237fc30 (pc 0x5558d237fc30 bp 0x7ff
#0 0x5558d237fc2f in computeOutputPixelOffsets /root/programs/libtiff/tools/tiffcrop.c:5802
#1 0x5558d236bd30 in main /root/programs/libtiff/tools/tiffcrop.c:2440
#2 0x7f26c9bc0bf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
#3 0x5558d2362869 in _start (/root/programs/libtiff/build_asan/bin/tiffcrop+0x28869)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE /root/programs/libtiff/tools/tiffcrop.c:5802 in computeOutputPixelOff
==390948==ABORTING
```

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_64
```

 [poc](#)

 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 \(#393\)](#)
1310



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

Activity



[Augustus @waugustus](#) · 8 months ago

Author

Contributor

Hi, I have analyzed the cause of this crash, as shown as follows,

Analysis

Crash cause

This crash happens in tiffcrop.c:5802

```
orows = TIFFhowmany(ilength, olength);

orows = (((uint32_t)(ilength))+((uint32_t)(olength)-1))/((uint32_t)(olength)); // From
```

We can use gdb to print the values

```
gdb-peda$ p ilength
$27 = 0x40
gdb-peda$ p olength
$28 = 0x0
```

We can see that olength=0, and this is the reason why the program crashes. From the code, we can find that olength is assigned in tiffcrop.c:5786

```
owidth = (uint32_t)(iwidth - (hmargin * 2 * page->hres));
olength = (uint32_t)(ilength - (vmargin * 2 * page->vres));
```

Use gdb to print values,

```
gdb-peda$ p vmargin
$32 = 0x0
gdb-peda$ p page->vres
$33 = -nan(0xe7d6420000000)
```

So the page->vres is **NaN** value, and it is an undefined behavior to convert a NaN to uint32_t

6.3.1.4 Real floating and integer

When a finite value of real floating type is converted to an integer type other than _Bool, the fractional part is discarded (i.e., the value is truncated toward zero). If the value of the integral part cannot be represented by the integer type, the behavior is undefined.⁵⁰

From the code, we can find that page->vres is assigned in tiffcrop.c:5700,

```
if (page->vres <= 1.0)
    page->vres = image->yres;
```

where image->yres is controlled by TIFFTAG_YRESOLUTION field.

So the crash cause is that the value in TIFFTAG_YRESOLUTION is a NaN, and the program does not check for it.

How to fix

We can add checks for INF and NaN in `tif_dir.c:342`, where the `image->yres` is assigned


```
// check for NaN and negative number
if( dblval != dblval || dblval < 0 )
    goto badvaluedouble;


// check for INF
if( val > FLT_MAX )
    dblval = FLT_MAX;
if( val < -FLT_MAX )
    dblval = -FLT_MAX;
```


Update: I think there may be no need to check for INF here, since the function `_TIFFClampDoubleToFloat(double val)` already does it.

```
float _TIFFClampDoubleToFloat( double val )
{
    if( val > FLT_MAX )
        return FLT_MAX;
    if( val < -FLT_MAX )
        return -FLT_MAX;
    return (float)val;
}
```

Edited by [4ugustus](#) 8 months ago

 [4ugustus](#) mentioned in merge request [!310 \(merged\)](#) 8 months ago

 [Even Rouault](#) mentioned in commit [f8d0f9aa](#) 8 months ago

 [Even Rouault](#) closed via merge request [!310 \(merged\)](#) 8 months ago

 [4ugustus](#) mentioned in commit [32ea0722](#) 8 months ago

 [Ozkan Sezer](#) mentioned in commit [freedesktop-sdk/mirrors/github/libsd1-org/SDL_image@19a9b461](#) 6 months ago

Please [register](#) or [sign in](#) to reply