Closed Issue created 5 months ago by 4ugustus

tiffcrop: FPE in computeOutputPixelOffsets, tiffcrop.c:5941

Summary

There is a FPE error in computeOutputPixelOffsets, tools/tiffcrop.c:5941. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted tiff file.

Version

LIBTIFF, Version 4.4.0, commit id 19db1d31 (Sun May 22 11:01:54 2022 +0200)

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 90 -H 300 -O landscape -P 300.0x300.0 -i poc /tmp/foo
TIFFReadDirectoryCheckOrder: Warning, Invalid TIFF directory; tags are not sorted in ascending order
TIFFReadDirectory: Warning, Unknown field with tag 65353 (0xff49) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 42 (0x2a) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 768 (0x300) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 52942 (0xcece) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 206 (0xce) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 22784 (0x5900) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 22873 (0x5959) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 89 (0x59) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 65378 (0xff62) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 0 (0x0) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 15677 (0x3d3d) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 22912 (0x5980) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 30041 (0x7559) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 65535 (0xffff) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 1024 (0x400) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 19836 (0x4d7c) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 24929 (0x6161) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 21081 (0x5259) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 1 (0x1) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 18761 (0x4949) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 23016 (0x59e8) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 22845 (0x593d) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 20569 (0x5059) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 31065 (0x7959) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 17241 (0x4359) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 22905 (0x5979) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 22869 (0x5955) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 23039 (0x59ff) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 514 (0x202) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 22872 (0x5958) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 23897 (0x5d59) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 22904 (0x5978) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 28 (0x1c) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 77 (0x4d) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 22897 (0x5971) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 22847 (0x593f) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 22617 (0x5859) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 15683 (0x3d43) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 18009 (0x4659) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 18777 (0x4959) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 59395 (0xe803) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 8281 (0x2059) encountered.
TIFFReadDirectory: Warning, Invalid data type for tag StripOffsets.
TIFFReadDirectory: Warning, Invalid data type for tag StripByteCounts.
TIFFFetchStripThing: Warning, Incorrect count for "StripOffsets"; tag ignored.
TIFFAdvanceDirectory: Error fetching directory count.
loadImage: Image lacks Photometric interpretation tag.
Fax3Decode1D: Warning, Premature EOL at line 0 of strip 0 (got 0, expected 7196).
```

```
Fax3Decode1D: Warning, Premature EOL at line 1 of strip 0 (got 116, expected 7196).
Fax3Decode1D: Warning, Premature EOL at line 2 of strip 0 (got 220, expected 7196).
Fax3Decode1D: Warning, Premature EOL at line 3 of strip 0 (got 11, expected 7196).
Fax3Decode1D: Warning, Premature EOL at line 4 of strip 0 (got 1856, expected 7196).
Fax3Decode1D: Warning, Premature EOL at line 5 of strip 0 (got 24, expected 7196).
Fax3Decode1D: Warning, Premature EOL at line 6 of strip 0 (got 105, expected 7196).
Fax3Decode1D: Warning, Premature EOL at line 7 of strip 0 (got 1854, expected 7196).
Fax3Decode1D: Warning, Premature EOL at line 8 of strip 0 (got 1664, expected 7196).
Fax3Decode1D: Warning, Premature EOL at line 9 of strip 0 (got 2306, expected 7196).
Fax3Decode1D: Warning, Premature EOL at line 10 of strip 0 (got 0, expected 7196).
Floating point exception (core dumped)

(gdb) # bt
#0  0x0000000000411835 in computeOutputPixelOffsets (crop=0x7fffffff8e70, image=0x7fffffff8bf0,
    page=0x7fffffff8c10, sections=0x7fffffff9160, dump=0x7fffffffb4f0) at tiffcrop.c:5941
#1  0x00000000004076d7 in main (argc=0xc, argv=0x7fffffffe648) at tiffcrop.c:2459
#2  0x00007ffff6749840 in __libc_start_main (main=0x406c6d <main>, argc=0xc, argv=0x7fffffffe648,
    init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffffe638)
    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

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 @waugustus · 5 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:5941

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

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

We can use gdb to print the values

```
gdb-peda$ p ilength
$27 = 0x59
gdb-peda$ 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)((pwidth * page->hres) - (hmargin * 2));
olength = (uint32_t)((plength * page->vres) - (vmargin * 2));
```

Use gdb to print values,

```
gdb-peda$ p plength
$5 = 300
gdb-peda$ p page->vres
$6 = 4294967296
gdb-peda$ p vmargin
$8 = 0x0
gdb-peda$ p ((plength * page->vres) - (vmargin * 2))
$9 = 1288490188800
```

Note that 1288490188800 = 0x12C**00000000**. Since the size of `uint32_t` is 4 bytes, convert such variable to `uint32_t` will get a zero-value.

How to fix

Create a `_TIFFClampDoubltToUInt32()` function to convert double to uint32_t,

```
uint32_t _TIFFClampDoubleToUInt32(double val)
{
    if( val < 0 )
        return 0;
    if( val > 0xFFFFFFFFU || val != val )
        return 0xFFFFFFFFU;
    return (uint32_t)val;
}
```

And add a check for `olength` and `owidth` in tiffcrop.c,

```
if (owidth == 0 || olength == 0)
{
    TIFFError("computeOutputPixelOffsets", "Integer overflow when calculating the number o
    exit(EXIT_FAILURE);
}
```

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