

# tiffcrop: FPE in computeOutputPixelOffsets, tiffcrop.c:5817

## Summary

There is a FPE error in computeOutputPixelOffsets, tools/tiffcrop.c:5817. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted tiff file.

## Version

LIBTIFF, Version 4.3.0, commit id [9752dae8](#) (Sat Apr 23 14:00:48 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 -R 270 -O auto -P 300.0x300.0 poc /tmp/foo
=====
==1710053==ERROR: AddressSanitizer: FPE on unknown address 0x5589ef8aeef4 (pc 0x5589ef8aeef4 bp 0x7f
#0 0x5589ef8aeef3 in computeOutputPixelOffsets /root/programs/libtiff/tools/tiffcrop.c:5818
#1 0x5589ef89af80 in main /root/programs/libtiff/tools/tiffcrop.c:2440
#2 0x7fab1a654c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
#3 0x5589ef891ab9 in _start (/root/programs/libtiff/build_asan/bin/tiffcrop+0x2bab9)


AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE /root/programs/libtiff/tools/tiffcrop.c:5818 in computeOutputPixelOff
==1710053==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_6
```

 [poc](#)

Edited 7 months ago by [Augustus](#)


 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 \(#415, #427, and #428\)](#)


1346




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


## Activity

 [Augustus](#) changed title from **FPE in computeOutputPixelOffsets, tiffcrop.c:5817** to **tiffcrop: FPE in computeOutputPixelOffsets, tiffcrop.c:5817** [7 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