Closed Issue created 6 months ago by **sheng peng**

tiffcrop: double free or corruption in rotateImage() at tiffcrop.c:8839

Summary

There is a double free or corruption in rotateImage() at tiffcrop.c:8839

```
8839: _TIFFfree(ibuff);
```

Version

```
root@peng:~/libtiff-v4.4.0rc1# tools/.libs/tiffcrop -v
Library Release: LIBTIFF, Version 4.4.0
Copyright (c) 1988-1996 Sam Leffler
Copyright (c) 1991-1996 Silicon Graphics, Inc.
Tiffcrop version: 2.5, last updated: 02-09-2022
```

Steps to reproduce

```
./autogen.sh
./configure
make -j
root@peng:~/libtiff-v4.4.0rc1# gdb --args tools/.libs/tiffcrop -Z 1:4,3:3 -R 90 -H 300 -S 2:2 -i poc
TIFFReadDirectory: Warning, Unknown field with tag 5467 (0x155b) encountered.
TIFFFetchNormalTag: Warning, IO error during reading of "Tag 5632"; tag ignored.
TIFFFetchNormalTag: Warning, Sanity check on size of "Tag 2" value failed; tag ignored.
TIFFFetchNormalTag: Warning, Incorrect count for "FillOrder"; tag ignored.
TIFFFetchNormalTag: Warning, IO error during reading of "YResolution"; tag ignored.
TIFFFetchNormalTag: Warning, incorrect count for field "YCbCrSubsampling", expected 2, got 335544322
TIFFReadDirectory: Warning, Wrong "StripByteCounts" field, ignoring and calculating from imagelength
double free or corruption (!prev)

Program received signal SIGABRT, Aborted.
__GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
51      ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) bt
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
#1  0x00007ffff77a17f1 in __GI_abort () at abort.c:79
#2  0x00007ffff77ea837 in __libc_message (action=action@entry=do_abort, fmt=fmt@entry=0x7ffff7917a7b
#3  0x00007ffff77f18ba in malloc_printerr (str=str@entry=0x7ffff79197a8 "double free or corruption (
#4  0x00007ffff77f8e5c in _int_free (have_lock=0, p=0x5555557706d0, av=0x7ffff7b4cc40 <main_arena>)
#5  __GI___libc_free (mem=0x5555557706e0) at malloc.c:3134
#6  0x000055555555be61 in rotateImage (rotation=<optimized out>, image=<optimized out>, img_width=0x
#7  0x00005555555568f6 in processCropSelections (read_buff_ptr=0x7fffffff8890, seg_buffs=0x7fffffff8
#8  main (argc=<optimized out>, argv=0x7fffffffe348) at tiffcrop.c:2415
```

Platform

uname -a Linux peng 5.4.0-42-generic 18.04.1-Ubuntu SMP Fri Jul 10 07:21:24 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux

poc2

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

tiffcrop: -S option mutually exclusive (fixes #349, #414, #422, #423, #424)

!378 ✓

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

Activity

- Su Laus mentioned in merge request !378 (merged) 3 months ago
- Even Rouault closed via merge request !378 (merged) 3 months ago
- Su Laus mentioned in commit `8fe37359` 3 months ago
- Even Rouault mentioned in commit `48d6ece8` 3 months ago

Please register or sign in to reply