

tiffcrop: free invalid pointer in TIFFClose() at tif_close.c:131 called by tiffcrop.c:2522

Summary

There is a invalid pointer free() operation in TIFFClose() at tif_close.c:131 called by tiffcrop.c:2522

```
131:TIFFCleanup(tif);
```

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
TIFFFetchDirectory: Can not read TIFF directory count.
TIFFReadDirectory: Failed to read directory at offset 4279506196.
free(): invalid pointer
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=0x7ffff7915c76 "free(): invalid pointer") a
#4  0x00007ffff77f8dec in _int_free (have_lock=0, p=0x55555576f730, av=0x7ffff7b4cc40 <main_arena>)
#5  __GI___libc_free (mem=0x55555576f740) at malloc.c:3134
#6  0x00007ffff7b5c9c9 in TIFFClose (tif=<optimized out>) at tif_close.c:131
#7  0x0000555555559487 in main (argc=<optimized out>, argv=0x7fffffe348) at tiffcrop.c:2522
```

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


 [poc1](#)

Edited 6 months ago by [sheng_peng](#)


 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

-  sheng.peng changed the description 6 months ago ·
-  Su Laus mentioned in 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
-  Even Rouault closed via merge request [!378 \(merged\)](#) 3 months ago

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