Closed Issue created 6 months ago by sheng peng

tiffcrop: sysmalloc assertion in rotateImage() at tiffcrop.c:8621

Summary

There is a sysmalloc assertion in rotateImage() at tiffcrop.c:8621

```
8621: if (!(rbuff = (unsigned char *)limitMalloc(buffsize)))
```

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
TIFFFillStrip: Read error on strip 20; got 18446744073708357672 bytes, expected 7304.
tiffcrop: malloc.c:2401: sysmalloc: Assertion `(old_top == initial_top (av) && old_size == 0) || ((u

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  0x00007ffff77f4af1 in __malloc_assert (file=<optimized out>, function=<optimized out>, line=<opt
#3  sysmalloc (nb=nb@entry=87680, av=av@entry=0x7ffff7b4cc40 <main_arena>) at malloc.c:2398
#4  0x00007ffff77f6060 in _int_malloc (av=av@entry=0x7ffff7b4cc40 <main_arena>, bytes=bytes@entry=87
#5  0x00007ffff77f80ac in __GI___libc_malloc (bytes=87660) at malloc.c:3067
#6  0x000055555555baa6 in rotateImage (rotation=<optimized out>, image=0x7fffffff88a0, img_width=0x7
    at tiffcrop.c:8621
#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

poc3

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