

/tools/tiffcrop.c:6866 - Heap use after free in extractImageSection

Summary

There is a Heap use after free vulnerability in /tools/tiffcrop.c:6866 in extractImageSection function. Similar issue has been raised for heap buffer overflow at the same location in the code. Looks like the previously freed memory is being referenced

Version

```
root@ubuntu:/home/tlibtiff/tools# ./tiffcrop -v
Library Release: LIBTIFF, Version 4.3.0
Copyright (c) 1988-1996 Sam Leffler
Copyright (c) 1991-1996 Silicon Graphics, Inc.
Tiffcrop version: 2.4, last updated: 12-13-2010
Tiffcp code: Copyright (c) 1988-1997 Sam Leffler
             : Copyright (c) 1991-1997 Silicon Graphics, Inc
Tiffcrop additions: Copyright (c) 2007-2010 Richard Nolde
```

Steps to reproduce - (How one can reproduce the issue - this is very important)

```
Clone the latest source from the gitlab repository - git clone https://gitlab.com/libtiff/libtiff.git
cd libtiff

compile the source using the following command :

CC=gcc CXX=g++ CFLAGS="-ggdb -fsanitize=address,undefined -fno-sanitize-recover=all" CXXFLAGS="-ggdb

Reproduce the crash with the following command :

./tiffcrop -i -E 1 -H 10 -V 10 -S 8:4 -R 270 poc.tif a.tif
```

Platform (Operating system, architecture, compiler details)

```
gcc --version
gcc (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0
Copyright (C) 2019 Free Software Foundation, Inc.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

uname -r
5.13.0-28-generic

uname -a
Linux ubuntu 5.13.0-28-generic #31~20.04.1-Ubuntu SMP Wed Jan 19 14:08:10 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux

lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.3 LTS
Release:        20.04
Codename:       focal
```

- Address Sanitizer Logs (ASAN)

```
TIFFReadDirectoryCheckOrder: Warning, Invalid TIFF directory; tags are not sorted in ascending order
TIFFReadDirectory: Warning, Unknown field with tag 60695 (0xed17) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 1 (0x1) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 0 (0x0) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 65535 (0xffff) encountered.
```

```

TIFFReadDirectory: Warning, Unknown field with tag 47308 (0xb8cc) encountered.
TIFFFetchNormalTag: Warning, incorrect count for field "PageNumber", expected 2, got 131075.
TIFFReadDirectory: Warning, Sum of Photometric type-related color channels and ExtraSamples doesn't
TIFFReadDirectory: Warning, TIFF directory is missing required "StripByteCounts" field, calculating
TIFFAdvanceDirectory: Error fetching directory count.
loadImage: Image lacks Photometric interpretation tag.
TIFFFillStrip: Read error on strip 0; got 18446744071562068202 bytes, expected 163200.
: Strip 1: read -1 bytes, strip size 163200.
TIFFFillStrip: Read error on strip 1; got 18446744071561905002 bytes, expected 163200.
: Strip 2: read -1 bytes, strip size 163200.
TIFFFillStrip: Read error on strip 2; got 18446744071561741802 bytes, expected 163200.
: Strip 3: read -1 bytes, strip size 163200.
TIFFFillStrip: Read error on strip 3; got 18446744071561578602 bytes, expected 163200.
: Strip 4: read -1 bytes, strip size 163200.
TIFFFillStrip: Read error on strip 4; got 18446744071561415402 bytes, expected 163200.
: Strip 5: read -1 bytes, strip size 163200.
TIFFFillStrip: Read error on strip 5; got 18446744071561252202 bytes, expected 163200.
: Strip 6: read -1 bytes, strip size 163200.
TIFFFillStrip: Read error on strip 6; got 18446744071561089002 bytes, expected 163200.
: Strip 7: read -1 bytes, strip size 163200.
TIFFFillStrip: Read error on strip 7; got 18446744071560925802 bytes, expected 163200.
: Strip 8: read -1 bytes, strip size 163200.
TIFFFillStrip: Read error on strip 8; got 18446744071560762602 bytes, expected 163200.
: Strip 9: read -1 bytes, strip size 163200.
TIFFFillStrip: Read error on strip 9; got 18446744071560599402 bytes, expected 163200.
=====
==3841220==ERROR: AddressSanitizer: heap-use-after-free on address 0x7f5bb2efad00 at pc 0x55b654278f
READ of size 1 at 0x7f5bb2efad00 thread T0
    #0 0x55b654278f2e in extractImageSection /home/targets/libtiff/tools/tiffcrop.c:6866
    #1 0x55b654278f2e in writeImageSections /home/targets/libtiff/tools/tiffcrop.c:7097
    #2 0x55b654278f2e in main /home/targets/libtiff/tools/tiffcrop.c:2451
    #3 0x7f5bb67f00b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #4 0x55b65427c4ed in _start (/home/targets/libtiff/tools/tiffcrop+0x324ed)


0x7f5bb2efad00 is located 120064 bytes inside of 1632010-byte region [0x7f5bb2edd800,0x7f5bb306bf0a)
freed by thread T0 here:
    #0 0x7f5bb6c337cf in __interceptor_free (/lib/x86_64-linux-gnu/libasan.so.5+0x10d7cf)
    #1 0x55b65428f35c in rotateImage /home/targets/libtiff/tools/tiffcrop.c:8697

previously allocated by thread T0 here:
    #0 0x7f5bb6c33bc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x55b65428e1c1 in rotateImage /home/targets/libtiff/tools/tiffcrop.c:8479

SUMMARY: AddressSanitizer: heap-use-after-free /home/targets/libtiff/tools/tiffcrop.c:6866 in extrac
Shadow bytes around the buggy address:
  0x0febf65d7550: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0febf65d7560: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0febf65d7570: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0febf65d7580: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0febf65d7590: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0febf65d75a0:[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0febf65d75b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0febf65d75c0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0febf65d75d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0febf65d75e0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0febf65d75f0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable:          00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:    fa
Freed heap region:    fd
Stack left redzone:   f1
Stack mid redzone:    f2
Stack right redzone:  f3
Stack after return:   f5
Stack use after scope: f8
Global redzone:       f9
Global init order:    f6
Poisoned by user:     f7
Container overflow:    fc
Array cookie:         ac
Intra object redzone: bb

```

```
ASan internal:      fe
Left alloca redzone: ca
Right alloca redzone: cb
Shadow gap:        cc
==3841220==ABORTING
[poc.zip](/uploads/3650065a674695ed1f9b89a01029bbfe/poc.zip)
```


 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: fix issue #380 and #382 heap buffer overflow in extractImageSection](#)
!307 

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

Activity



[Chintan Shah](#) @shahcs · 9 months ago

Author

 [poc.zip](#)



[Su Laus](#) mentioned in merge request [!307 \(merged\)](#) 9 months ago



[Even Rouault](#) mentioned in commit [46dc8fcd](#) 8 months ago



[Su Laus](#) closed via commit [232282fd](#) 8 months ago



[Even Rouault](#) closed via merge request [!307 \(merged\)](#) 8 months ago



[Su Laus](#) mentioned in commit [freedesktop-sdk/mirrors/gitlab/libtiff/libtiff@232282fd](#) 8 months ago

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