

tiffcrop: heap-buffer-overflow in extractImageSection, tiffcrop.c:6905

Summary

There is a heap buffer overflow in extractImageSection in tools/tiffcrop.c:6905. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted tiff file. Note that it is different from [#349 \(closed\)](#).

Version

LIBTIFF, Version 4.3.0, commit id [b51bb157](#) (Mon Mar 21 18:03:17 2022 +0100)

Steps to reproduce

```
# CFLAGS="-g -fsanitize=address -fno-omit-frame-pointer" CXXFLAGS="-g -fsanitize=address -fno-omit-frame-pointer"

# make -j; make install; make clean

# ./build_asan/bin/tiffcrop -Z 1:4,3:3 -R 90 -H 300 -S 2:2 -i poc /tmp/foo
TIFFReadDirectoryCheckOrder: Warning, Invalid TIFF directory; tags are not sorted in ascending order
TIFFReadDirectory: Warning, Unknown field with tag 2 (0x2) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 48 (0x30) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 8832 (0x2280) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 6400 (0x1900) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 62085 (0xf285) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 0 (0x0) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 65484 (0xffcc) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 1 (0x1) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 6 (0x6) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 15626 (0x3d0a) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 384 (0x180) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 22784 (0x5900) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 20480 (0x5000) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 22528 (0x5800) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 8192 (0x2000) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 23552 (0x5c00) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 27487 (0x6b5f) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 200 (0xc8) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 32803 (0x8023) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 52224 (0xcc00) encountered.
TIFFFetchNormalTag: Warning, IO error during reading of "Tag 6400"; tag ignored.
TIFFFetchNormalTag: Warning, Sanity check on size of "Tag 15626" value failed; tag ignored.
TIFFFetchNormalTag: Warning, ASCII value for tag "DocumentName" contains null byte in value; value ignored.
TIFFFetchNormalTag: Warning, Incompatible type for "YResolution"; tag ignored.
TIFFFetchNormalTag: Warning, Incorrect count for "ResolutionUnit"; tag ignored.
TIFFFetchNormalTag: Warning, IO error during reading of "Tag 20480"; tag ignored.
TIFFFetchNormalTag: Warning, IO error during reading of "Tag 22528"; tag ignored.
TIFFReadDirectory: Warning, Sum of Photometric type-related color channels and ExtraSamples doesn't match
TIFFReadDirectory: Warning, Bogus "StripByteCounts" field, ignoring and calculating from imagelength
TIFFAdvanceDirectory: Error fetching directory count.
loadImage: Image lacks Photometric interpretation tag.
TIFFFillStrip: Read error on strip 0; got 672 bytes, expected 1142418.
=====
==3975482==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7fc9373ff695 at pc 0x55d0a9e2b2b9
READ of size 1 at 0x7fc9373ff695 thread T0
#0 0x55d0a9e2bd31 in extractImageSection /root/programs/libtiff/tools/tiffcrop.c:6905
#1 0x55d0a9e2ceb3 in writeImageSections /root/programs/libtiff/tools/tiffcrop.c:7093
#2 0x55d0a9e130c8 in main /root/programs/libtiff/tools/tiffcrop.c:2451
#3 0x7fc93aa5ec86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
#4 0x55d0a9e09ab9 in _start (/root/programs/libtiff/build_asan/bin/tiffcrop+0x2bab9)

0x7fc9373ff695 is located 0 bytes to the right of 1142421-byte region [0x7fc9372e8800,0x7fc9373ff695)
allocated by thread T0 here:
#0 0x7fc93c097b40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
#1 0x55d0a9ea5a77 in _TIFFMalloc /root/programs/libtiff/libtiff/tif_unix.c:314
#2 0x55d0a9e09c6d in limitMalloc /root/programs/libtiff/tools/tiffcrop.c:627
#3 0x55d0a9e290b9 in loadImage /root/programs/libtiff/tools/tiffcrop.c:6220
#4 0x55d0a9e129ae in main /root/programs/libtiff/tools/tiffcrop.c:2374
```


```
#5 0x7fc93aa5ec86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)


SUMMARY: AddressSanitizer: heap-buffer-overflow /root/programs/libtiff/tools/tiffcrop.c:6905 in extr
Shadow bytes around the buggy address:
  0x0ff9a6e77e80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff9a6e77e90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff9a6e77ea0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff9a6e77eb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff9a6e77ec0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0ff9a6e77ed0: 00 00[05]fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff9a6e77ee0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff9a6e77ef0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff9a6e77f00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff9a6e77f10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff9a6e77f20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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
==3975482==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_64
```

 [poc](#)


 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 \(fixes #349, #414, #422, #423, #424\)](#)

1378



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

Activity

 [Su Laus](#) mentioned in merge request [1378 \(merged\)](#) 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