Closed Issue created 7 months ago by 4ugustus

tiffcrop: heap-buffer-overflow in _TIFFmemcpy, tif_unix.c:346 (different from #411)

Summary

There is a heap buffer overflow in _TIFFmemcpy in libtiff/tif_unix.c:346. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted tiff file.

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-f

# make -j; make install; make clean

# ./build_asan/bin/tiffcrop -Z 1:4,3:3 -R 90 -H 300 -i poc /tmp/foo
IFFReadDirectoryCheckOrder: 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 4617 (0x1209) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 6656 (0x1a00) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 62085 (0xf285) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 8240 (0x2030) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 31350 (0x7a76) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 59310 (0xe7ae) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 15904 (0x3e20) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 15626 (0x3d0a) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 2313 (0x909) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 29812 (0x7474) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 27137 (0x6a01) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 65396 (0xff74) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 24014 (0x5dce) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 10088 (0x2768) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 31868 (0x7c7c) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 0 (0x0) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 18761 (0x4949) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 61695 (0xf0ff) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 52224 (0xcc00) encountered.
TIFFFetchNormalTag: Warning, Incorrect count for "PhotometricInterpretation"; 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 i
TIFFFetchNormalTag: Warning, Incorrect count for "YResolution"; tag ignored.
TIFFReadDirectory: Warning, Ignoring ColorMap since BitsPerSample tag not found.
TIFFReadDirectory: Warning, Sum of Photometric type-related color channels and ExtraSamples doesn't
TIFFAdvanceDirectory: Error fetching directory link.
loadImage: Image lacks Photometric interpretation tag.
LZWPreDecode: Warning, Old-style LZW codes, convert file.
output_tiffcrop_random_3/default/crashes/id:000000,sig:11,src:003379,time:11040083,execs:8056393,op:
=================================================================
==1900940==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7fb6375ff457 at pc 0x7fb63c2b7
READ of size 112648 at 0x7fb6375ff457 thread T0
    #0 0x7fb63c2b7732  (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x79732)
    #1 0x561892042b49 in _TIFFmemcpy /root/programs/libtiff/libtiff/tif_unix.c:346
    #2 0x561891fc8b24 in extractImageSection /root/programs/libtiff/tools/tiffcrop.c:6826
    #3 0x561891fc9eb3 in writeImageSections /root/programs/libtiff/tools/tiffcrop.c:7093
    #4 0x561891fb00c8 in main /root/programs/libtiff/tools/tiffcrop.c:2451
    #5 0x7fb63ace3c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #6 0x561891fa6ab9 in _start (/root/programs/libtiff/build_asan/bin/tiffcrop+0x2bab9)

0x7fb6375ff457 is located 0 bytes to the right of 1182807-byte region [0x7fb6374de800,0x7fb6375ff457
allocated by thread T0 here:
    #0 0x7fb63c31cb40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x561892042a77 in _TIFFmalloc /root/programs/libtiff/libtiff/tif_unix.c:314
    #2 0x561891fa6c6d in limitMalloc /root/programs/libtiff/tools/tiffcrop.c:627
    #3 0x561891fc60b9 in loadImage /root/programs/libtiff/tools/tiffcrop.c:6220
    #4 0x561891faf9ae in main /root/programs/libtiff/tools/tiffcrop.c:2374
    #5 0x7fb63ace3c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x79732)
Shadow bytes around the buggy address:
  0x0ff746eb7e30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff746eb7e40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff746eb7e50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff746eb7e60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff746eb7e70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0ff746eb7e80: 00 00 00 00 00 00 00 00 00 00[07]fa fa fa fa fa
  0x0ff746eb7e90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff746eb7ea0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff746eb7eb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff746eb7ec0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff746eb7ed0: 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
==1900940==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_6
```

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: disable incompatibility of -Z, -X, -Y, -z options with any PAGE_MODE_x option (fixes #411, #413 an...
!383 ✓

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

Activity

Su Laus mentioned in merge request !383 (merged) 3 months ago

Even Rouault closed via commit 236b7191 1 month ago

Su Laus mentioned in commit Su_Laus/test@4746f162 1 month ago

Even Rouault mentioned in commit Su_Laus/test@236b7191 1 month ago

Please register or sign in to reply