Closed Issue created 8 months ago by **4ugustus**

tiffcrop: heap-buffer-overflow in _TIFFmemcpy, tif_unix.c:346

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 5e180045 (Fri Feb 25 10:38:31 2022 +0000)

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 -H 341 poc /tmp/foo

TIFFReadDirectoryCheckOrder: Warning, Invalid TIFF directory; tags are not sorted in ascending order
TIFFReadDirectory: Warning, Unknown field with tag 9216 (0x2400) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 0 (0x0) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 501 (0x1f5) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 292 (0x124) encountered.
TIFFFetchNormalTag: Warning, ASCII value for tag "InkNames" does not end in null byte. Forcing it to
TIFFSetField: poc_tiffcrop/00003: Invalid InkNames value; expecting 1281 names, found 1.
TIFFFetchNormalTag: Warning, IO error during reading of "Tag 501"; tag ignored.
TIFFFetchNormalTag: Warning, Incompatible type for "NumberOfInks"; tag ignored.
TIFFFetchNormalTag: Warning, Incompatible type for "Orientation"; tag ignored.
TIFFReadDirectory: Warning, Sum of Photometric type-related color channels and ExtraSamples doesn't
TIFFAdvanceDirectory: Error fetching directory count.
loadImage: Image lacks Photometric interpretation tag.
Fax4Decode: Warning, Line length mismatch at line 0 of strip 0 (got 21, expected 20).
Fax4Decode: Warning, Line length mismatch at line 1 of strip 0 (got 26, expected 20).
Fax4Decode: Warning, Line length mismatch at line 2 of strip 0 (got 26, expected 20).
Fax4Decode: Warning, Line length mismatch at line 3 of strip 0 (got 26, expected 20).
Fax4Decode: Warning, Line length mismatch at line 4 of strip 0 (got 21, expected 20).
Fax4Decode: Warning, Line length mismatch at line 5 of strip 0 (got 913, expected 20).
Fax4Decode: Warning, Line length mismatch at line 6 of strip 0 (got 26, expected 20).
Fax4Decode: Warning, Line length mismatch at line 7 of strip 0 (got 27, expected 20).
Fax4Decode: Warning, Line length mismatch at line 8 of strip 0 (got 49, expected 20).
Fax4Decode: Warning, Line length mismatch at line 10 of strip 0 (got 25, expected 20).
Fax4Decode: Warning, Line length mismatch at line 14 of strip 0 (got 21, expected 20).
Fax4Decode: Bad code word at line 21 of strip 0 (x 0).
Fax4Decode: Warning, Premature EOL at line 21 of strip 0 (got 0, expected 20).
=================================================================
==1931320==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f54f2e679e3 at pc 0x7f54f1deb
READ of size 3202 at 0x7f54f2e679e3 thread T0
    #0 0x7f54f1deb732  (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x79732)
    #1 0x55b80c4a7831 in _TIFFmemcpy /root/programs/libtiff/libtiff/tif_unix.c:346
    #2 0x55b80c42d8c5 in extractImageSection /root/programs/libtiff/tools/tiffcrop.c:6854
    #3 0x55b80c42ec8f in writeImageSections /root/programs/libtiff/tools/tiffcrop.c:7103
    #4 0x55b80c414e78 in main /root/programs/libtiff/tools/tiffcrop.c:2451
    #5 0x7f54f0d4bbf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
    #6 0x55b80c40b869 in _start (/root/programs/libtiff/build_asan/bin/tiffcrop+0x28869)

0x7f54f2e679e3 is located 0 bytes to the right of 512483-byte region [0x7f54f2dea800,0x7f54f2e679e3)
allocated by thread T0 here:
    #0 0x7f54f1e50b40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x55b80c4a775f in _TIFFmalloc /root/programs/libtiff/libtiff/tif_unix.c:314
    #2 0x55b80c40ba1d in limitMalloc /root/programs/libtiff/tools/tiffcrop.c:627
    #3 0x55b80c42adab in loadImage /root/programs/libtiff/tools/tiffcrop.c:6210
    #4 0x55b80c41475e in main /root/programs/libtiff/tools/tiffcrop.c:2374
    #5 0x7f54f0d4bbf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x79732)
Shadow bytes around the buggy address:
  0x0feb1e5c4ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0feb1e5c4ef0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0feb1e5c4f00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0feb1e5c4f10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0feb1e5c4f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0feb1e5c4f30: 00 00 00 00 00 00 00 00 00 00 00 00 00[03]fa fa fa
  0x0feb1e5c4f40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0feb1e5c4f50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0feb1e5c4f60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0feb1e5c4f70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0feb1e5c4f80: 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
==1931320==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

Edited 8 months ago by 4ugustus

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

Activity

4ugustus @waugustus · 8 months ago Author Contributor

Analysis

Crash cause

When we print the backtrace with gdb, we can see that the dest_addr and src_addr in memcpy are 0x7ffff6b28188 and 0x7ffff7ba8888, respectively.

```
gdb-peda$ bt
#0  __memmove_avx_unaligned_erms () at ../sysdeps/x86_64/multiarch/memmove-vec-unaligned-e
#1  0x000055555559a285 in _TIFFmemcpy (d=0x7ffff6b28188, s=0x7ffff7ba8888, c=0x1fe0) at ti
#2  0x000055555556ab4f in extractImageSection (image=0x7fffffff8f00, section=0x7fffffff947
#3  0x000055555556b459 in writeImageSections (in=0x555555617eb0, out=0x55555561b240, image
    src_buff=0x7ffff7430010 "", sect_buff_ptr=0x7fffffff8ed8) at tiffcrop.c:7103
#4  0x000055555555ece4 in main (argc=0x5, argv=0x7fffffffe968) at tiffcrop.c:2451
#5  0x00007ffff77b90b3 in __libc_start_main (main=0x55555555e166 <main>, argc=0x5, argv=0x
    at ../csu/libc-start.c:308
#6  0x000055555555a26e in _start ()
```

We can print the memory layout as shown as follows,

~~~~
```
Start              End                Perm      Name
0x0000555555554000 0x0000555555559000 r--p      /home/data/wdw/programs/libtiff/build_o
rig/bin/tiffcrop
0x0000555555559000 0x00005555555cc000 r-xp      /home/data/wdw/programs/libtiff/build_o
rig/bin/tiffcrop
0x00005555555cc000 0x0000555555600000 r--p      /home/data/wdw/programs/libtiff/build_o
rig/bin/tiffcrop
0x0000555555600000 0x0000555555605000 r--p      /home/data/wdw/programs/libtiff/build_o
rig/bin/tiffcrop
0x0000555555605000 0x0000555555606000 rw-p      /home/data/wdw/programs/libtiff/build_o
rig/bin/tiffcrop
0x0000555555606000 0x000055555565a000 rw-p      [heap]
0x00007ffff6a39000 0x00007ffff7573000 rw-p      mapped
0x00007ffff7573000 0x00007ffff7576000 r--p      /usr/lib/x86_64-linux-gnu/libgcc_s.so.1
0x00007ffff7576000 0x00007ffff7588000 r-xp      /usr/lib/x86_64-linux-gnu/libgcc_s.so.1
0x00007ffff7588000 0x00007ffff758c000 r--p      /usr/lib/x86_64-linux-gnu/libgcc_s.so.1
0x00007ffff758c000 0x00007ffff758d000 r--p      /usr/lib/x86_64-linux-gnu/libgcc_s.so.1
0x00007ffff758d000 0x00007ffff758e000 rw-p      /usr/lib/x86_64-linux-gnu/libgcc_s.so.1
0x00007ffff758e000 0x00007ffff7590000 rw-p      mapped
0x00007ffff7590000 0x00007ffff7626000 r--p      /usr/lib/x86_64-linux-gnu/libstdc++.so.
6.0.28
0x00007ffff7626000 0x00007ffff7717000 r-xp      /usr/lib/x86_64-linux-gnu/libstdc++.so.
6.0.28
0x00007ffff7717000 0x00007ffff7760000 r--p      /usr/lib/x86_64-linux-gnu/libstdc++.so.
6.0.28
0x00007ffff7760000 0x00007ffff7761000 ---p      /usr/lib/x86_64-linux-gnu/libstdc++.so.
6.0.28
0x00007ffff7761000 0x00007ffff776c000 r--p      /usr/lib/x86_64-linux-gnu/libstdc++.so.
6.0.28
0x00007ffff776c000 0x00007ffff776f000 rw-p      /usr/lib/x86_64-linux-gnu/libstdc++.so.
6.0.28
0x00007ffff776f000 0x00007ffff7772000 rw-p      mapped
0x00007ffff7772000 0x00007ffff7778000 r--p      /usr/lib/x86_64-linux-gnu/libpthread-2.
31.so
0x00007ffff7778000 0x00007ffff7789000 r-xp      /usr/lib/x86_64-linux-gnu/libpthread-2.
31.so
0x00007ffff7789000 0x00007ffff778f000 r--p      /usr/lib/x86_64-linux-gnu/libpthread-2.
31.so
0x00007ffff778f000 0x00007ffff7790000 r--p      /usr/lib/x86_64-linux-gnu/libpthread-2.
31.so
0x00007ffff7790000 0x00007ffff7791000 rw-p      /usr/lib/x86_64-linux-gnu/libpthread-2.
31.so
0x00007ffff7791000 0x00007ffff7795000 rw-p      mapped
0x00007ffff7795000 0x00007ffff77b7000 r--p      /usr/lib/x86_64-linux-gnu/libc-2.31.so
0x00007ffff77b7000 0x00007ffff792f000 r-xp      /usr/lib/x86_64-linux-gnu/libc-2.31.so
0x00007ffff792f000 0x00007ffff797d000 r--p      /usr/lib/x86_64-linux-gnu/libc-2.31.so
0x00007ffff797d000 0x00007ffff7981000 r--p      /usr/lib/x86_64-linux-gnu/libc-2.31.so
0x00007ffff7981000 0x00007ffff7983000 rw-p      /usr/lib/x86_64-linux-gnu/libc-2.31.so
0x00007ffff7983000 0x00007ffff7987000 rw-p      mapped
0x00007ffff7987000 0x00007ffff7994000 r--p      /usr/lib/x86_64-linux-gnu/libm-2.31.so
0x00007ffff7994000 0x00007ffff7a3b000 r-xp      /usr/lib/x86_64-linux-gnu/libm-2.31.so
0x00007ffff7a3b000 0x00007ffff7ad4000 r--p      /usr/lib/x86_64-linux-gnu/libm-2.31.so
0x00007ffff7ad4000 0x00007ffff7ad5000 r--p      /usr/lib/x86_64-linux-gnu/libm-2.31.so
~~~~

```
0x00007ffff7ad5000 0x00007ffff7ad6000 rw-p      /usr/lib/x86_64-linux-gnu/libm-2.31.so
0x00007ffff7ad6000 0x00007ffff7ad8000 r--p      /usr/lib/x86_64-linux-gnu/libz.so.1.2.11
0x00007ffff7ad8000 0x00007ffff7ae9000 r-xp      /usr/lib/x86_64-linux-gnu/libz.so.1.2.11
0x00007ffff7ae9000 0x00007ffff7aef000 r--p      /usr/lib/x86_64-linux-gnu/libz.so.1.2.11
0x00007ffff7aef000 0x00007ffff7af0000 ---p      /usr/lib/x86_64-linux-gnu/libz.so.1.2.11
0x00007ffff7af0000 0x00007ffff7af1000 r--p      /usr/lib/x86_64-linux-gnu/libz.so.1.2.11
0x00007ffff7af1000 0x00007ffff7af2000 rw-p      /usr/lib/x86_64-linux-gnu/libz.so.1.2.11
0x00007ffff7af2000 0x00007ffff7af3000 r--p      /usr/lib/x86_64-linux-gnu/libdeflate.so.0
0x00007ffff7af3000 0x00007ffff7b0a000 r-xp      /usr/lib/x86_64-linux-gnu/libdeflate.so.0
0x00007ffff7b0a000 0x00007ffff7b0e000 r--p      /usr/lib/x86_64-linux-gnu/libdeflate.so.0
0x00007ffff7b0e000 0x00007ffff7b0f000 r--p      /usr/lib/x86_64-linux-gnu/libdeflate.so.0
0x00007ffff7b0f000 0x00007ffff7b10000 rw-p      /usr/lib/x86_64-linux-gnu/libdeflate.so.0
0x00007ffff7b10000 0x00007ffff7b12000 rw-p      mapped
0x00007ffff7b12000 0x00007ffff7b16000 r--p      /usr/lib/x86_64-linux-gnu/libjpeg.so.8.2.2
0x00007ffff7b16000 0x00007ffff7b5a000 r-xp      /usr/lib/x86_64-linux-gnu/libjpeg.so.8.2.2
0x00007ffff7b5a000 0x00007ffff7b94000 r--p      /usr/lib/x86_64-linux-gnu/libjpeg.so.8.2.2
0x00007ffff7b94000 0x00007ffff7b95000 ---p      /usr/lib/x86_64-linux-gnu/libjpeg.so.8.2.2
0x00007ffff7b95000 0x00007ffff7b96000 r--p      /usr/lib/x86_64-linux-gnu/libjpeg.so.8.2.2
0x00007ffff7b96000 0x00007ffff7b97000 rw-p      /usr/lib/x86_64-linux-gnu/libjpeg.so.8.2.2
0x00007ffff7b97000 0x00007ffff7ba2000 r-xp      /usr/lib/x86_64-linux-gnu/libjbig.so.0
0x00007ffff7ba2000 0x00007ffff7da1000 ---p      /usr/lib/x86_64-linux-gnu/libjbig.so.0
0x00007ffff7da1000 0x00007ffff7da2000 r--p      /usr/lib/x86_64-linux-gnu/libjbig.so.0
0x00007ffff7da2000 0x00007ffff7da5000 rw-p      /usr/lib/x86_64-linux-gnu/libjbig.so.0
0x00007ffff7da5000 0x00007ffff7ddb000 r--p      /usr/local/lib/libLerc.so.3
0x00007ffff7ddb000 0x00007ffff7e5e000 r-xp      /usr/local/lib/libLerc.so.3
0x00007ffff7e5e000 0x00007ffff7e72000 r--p      /usr/local/lib/libLerc.so.3
0x00007ffff7e72000 0x00007ffff7e73000 r--p      /usr/local/lib/libLerc.so.3
0x00007ffff7e73000 0x00007ffff7e77000 rw-p      /usr/local/lib/libLerc.so.3
0x00007ffff7e77000 0x00007ffff7e7a000 r--p      /usr/lib/x86_64-linux-gnu/liblzma.so.5.2.4
0x00007ffff7e7a000 0x00007ffff7e92000 r-xp      /usr/lib/x86_64-linux-gnu/liblzma.so.5.2.4
0x00007ffff7e92000 0x00007ffff7e9d000 r--p      /usr/lib/x86_64-linux-gnu/liblzma.so.5.2.4
0x00007ffff7e9d000 0x00007ffff7e9e000 ---p      /usr/lib/x86_64-linux-gnu/liblzma.so.5.2.4
0x00007ffff7e9e000 0x00007ffff7e9f000 r--p      /usr/lib/x86_64-linux-gnu/liblzma.so.5.2.4
0x00007ffff7e9f000 0x00007ffff7ea0000 rw-p      /usr/lib/x86_64-linux-gnu/liblzma.so.5.2.4
0x00007ffff7ea0000 0x00007ffff7ea4000 r--p      /usr/lib/x86_64-linux-gnu/libzstd.so.1.4.4
0x00007ffff7ea4000 0x00007ffff7f36000 r-xp      /usr/lib/x86_64-linux-gnu/libzstd.so.1.4.4
0x00007ffff7f36000 0x00007ffff7f47000 r--p      /usr/lib/x86_64-linux-gnu/libzstd.so.1.4.4
0x00007ffff7f47000 0x00007ffff7f48000 r--p      /usr/lib/x86_64-linux-gnu/libzstd.so.1.4.4
0x00007ffff7f48000 0x00007ffff7f49000 rw-p      /usr/lib/x86_64-linux-gnu/libzstd.so.1.4.4
0x00007ffff7f49000 0x00007ffff7f4b000 r--p      /usr/lib/x86_64-linux-gnu/libwebp.so.6.0.2
0x00007ffff7f4b000 0x00007ffff7f9c000 r-xp      /usr/lib/x86_64-linux-gnu/libwebp.so.6.0.2
0x00007ffff7f9c000 0x00007ffff7faf000 r--p      /usr/lib/x86_64-linux-gnu/libwebp.so.6.
```

~~~
0.2
0x00007ffff7faf000 0x00007ffff7fb0000 r--p      /usr/lib/x86_64-linux-gnu/libwebp.so.6.
0.2
0x00007ffff7fb0000 0x00007ffff7fb1000 rw-p      /usr/lib/x86_64-linux-gnu/libwebp.so.6.
0.2
0x00007ffff7fb1000 0x00007ffff7fb5000 rw-p      mapped
0x00007ffff7fc9000 0x00007ffff7fcd000 r--p      [vvar]
0x00007ffff7fcd000 0x00007ffff7fcf000 r-xp      [vdso]
0x00007ffff7fcf000 0x00007ffff7fd0000 r--p      /usr/lib/x86_64-linux-gnu/ld-2.31.so
0x00007ffff7fd0000 0x00007ffff7ff3000 r-xp      /usr/lib/x86_64-linux-gnu/ld-2.31.so
0x00007ffff7ff3000 0x00007ffff7ffb000 r--p      /usr/lib/x86_64-linux-gnu/ld-2.31.so
0x00007ffff7ffb000 0x00007ffff7ffc000 r--s      /home/data/wdw/programs/libtiff/poc_tif
fcrop/00001
0x00007ffff7ffc000 0x00007ffff7ffd000 r--p      /usr/lib/x86_64-linux-gnu/ld-2.31.so
0x00007ffff7ffd000 0x00007ffff7ffe000 rw-p      /usr/lib/x86_64-linux-gnu/ld-2.31.so
0x00007ffff7ffe000 0x00007ffff7fff000 rw-p      mapped
0x00007ffffffde000 0x00007ffffffff000 rw-p      [stack]
0xffffffffff600000 0xffffffffff601000 --xp      [vsyscall]
```
~~~

It seems that the src_addr (0x7ffff7ba8888) is in a unreadable area (---p). The program tries to read the contents of this area, so it crashes. In summary, it's **an out-of-bounds read error.**

How to fix

I think it is useful to add checks for memory bounds. From the code, read_buff is allocated *buffsize* bytes of memory in tiffcrop.c:6210 (i.e., src_buff). And the *buffersize* is equal to

```
if (TIFFIsTiled(in)) {
    tlsize = TIFFTileSize(in);
    ntiles = TIFFNumberOfTiles(in);
    buffsize = tlsize * ntiles;
}
else
{
    stsize = TIFFStripSize(in);
    nstrips = TIFFNumberOfStrips(in);
    buffsize = stsize * nstrips;
}
```

Also, sect_buff is allocated *sectsize* bytes of memory for each section in tiff crop.c:7096., where the *sectsize* is

```
width  = sections[i].x2 - sections[i].x1 + 1;
length = sections[i].y2 - sections[i].y1 + 1;
sectsize = (uint32_t) ceil((width * image->bps + 7) / (double)8) * image->spp * length;
```

For the code in tiffcrop.c:6854,

```
_TIFFmemcpy (sect_buff + dst_offset, src_buff + offset1, full_bytes);
```

there are four kinds of potential overflow errors,

1. full_bytes > sectsize - dst_offset
2. dst_offset > sectsize
3. full_bytes > buffsize - offset1
4. src_buff > offset1

the *full_bytes* is equal to

```
first_row = section->y1;
last_row  = section->y2;
first_col = section->x1;
last_col  = section->x2;

sect_width = last_col - first_col + 1;
full_bytes = (sect_width * spp * bps) / 8;
```

It is easy to add checks for the first two errors in extractImageSection, tiffcrop.c:6854, since *section* and *image* are passed into this function. But I have no idea how to add checks for the latter two errors, as we cannot get the pointer of *in* (or *tif*) in this function so that we cannot calculate the *buffsize*.

4ugustus changed the description 8 months ago ·

4ugustus @waugustus · 8 months ago Author Contributor

fixed by !307 (merged)

4ugustus closed 8 months ago

Please register or sign in to reply