Closed Issue created 11 months ago by p870613

heap-buffer-overflow /home/lin/libtiff/tools/tiffinfo.c:440:8 in TIFFReadRawDataStriped in branch 27f399af

Summary heap-buffer-overflow /home/lin/libtiff/tools/tiffinfo.c:440:8 in TIFFReadRawDataStriped

(Summarize the bug encountered concisely)

Version

```
➜  tiffinfo_test git:(master) ✗ ./tiffinfo -v
LIBTIFF, Version 4.3.0
Copyright (c) 1988-1996 Sam Leffler
Copyright (c) 1991-1996 Silicon Graphics, Inc.
```

(libtiff version)

Steps to reproduce

```
git clone git@gitlab.com:libtiff/libtiff.git
cd libtiff/
./autogen.sh
./configure CC=gcc CXX=g++ CFLAGS="-g -fsanitize=address" --disable-shared & make
./tools/tiffinfo -D -i  -r ./poc
```

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

Platform

```
➜  libtiff git:(master) ✗ gcc --version
gcc (Ubuntu 7.5.0-3ubuntu1~18.04) 7.5.0
Copyright (C) 2017 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.

➜  libtiff git:(master) ✗ uname -r
5.4.0-91-generic
➜  libtiff git:(master) ✗ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.5 LTS
Release:        18.04
Codename:       bionic
```

(Operating system, architecture, compiler details)

```
➜  libtiff git:(master) ✗ ./tools/tiffinfo -D -i  -r ./poc
TIFFReadDirectoryCheckOrder: Warning, Invalid TIFF directory; tags are not sorted in ascending order
TIFFReadDirectory: Warning, Unknown field with tag 21 (0x15) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 313 (0x139) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 6912 (0x1b00) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 24576 (0x6000) encountered.
TIFFFetchNormalTag: Warning, IO error during reading of "DocumentName"; tag ignored.
TIFFFetchNormalTag: Warning, incorrect count for field "YCbCrSubsampling", expected 2, got 429496727
TIFFReadDirectory: Warning, Photometric tag is missing, assuming data is YCbCr.
TIFFReadDirectory: Warning, SamplesPerPixel tag is missing, applying correct SamplesPerPixel value o
=== TIFF directory 0 ===
TIFF Directory at offset 0x62 (98)
  Image Width: 32 Image Length: 32
  Resolution: 0.0138889, 5.00784 (unitless)
  Bits/Sample: 4
  Compression Scheme: Old-style JPEG
  Photometric Interpretation: YCbCr
  FillOrder: msb-to-lsb
  YCbCr Subsampling: 2, 2
  Samples/Pixel: 3
  Rows/Strip: 32
  Planar Configuration: separate image planes
  Tag 21: 8646911286195530313
  Tag 313: 20480,1
TIFFReadRawStrip: Compression scheme does not support access to raw uncompressed data.
Error reading strip 0
=================================================================
==15842==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000118 at pc 0x55852c7268e
READ of size 8 at 0x602000000118 thread T0
    #0 0x55852c7268e3 in TIFFReadRawDataStriped /home/lin/libtiff/tools/tiffinfo.c:440
    #1 0x55852c7272ee in TIFFReadRawData /home/lin/libtiff/tools/tiffinfo.c:530
    #2 0x55852c72748d in tiffinfo /home/lin/libtiff/tools/tiffinfo.c:547
    #3 0x55852c72493a in main /home/lin/libtiff/tools/tiffinfo.c:160
    #4 0x7f277f78fbf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
    #5 0x55852c724199 in _start (/home/lin/libtiff/tools/tiffinfo+0x25199)

0x602000000118 is located 0 bytes to the right of 8-byte region [0x602000000110,0x602000000118)
allocated by thread T0 here:
    #0 0x7f2780894b40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x55852c788fdf in _TIFFmalloc /home/lin/libtiff/libtiff/tif_unix.c:314
    #2 0x55852c750f22 in TIFFReadDirEntryLong8ArrayWithLimit /home/lin/libtiff/libtiff/tif_dirread.c
    #3 0x55852c7687fb in TIFFFetchStripThing /home/lin/libtiff/libtiff/tif_dirread.c:5744
    #4 0x55852c75bebe in TIFFReadDirectory /home/lin/libtiff/libtiff/tif_dirread.c:4071
    #5 0x55852c76f707 in TIFFClientOpen /home/lin/libtiff/libtiff/tif_open.c:484
    #6 0x55852c788d45 in TIFFFdOpen /home/lin/libtiff/libtiff/tif_unix.c:209
    #7 0x55852c788f9e in TIFFOpen /home/lin/libtiff/libtiff/tif_unix.c:248
    #8 0x55852c7247f5 in main /home/lin/libtiff/tools/tiffinfo.c:147
    #9 0x7f277f78fbf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/lin/libtiff/tools/tiffinfo.c:440 in TIFFReadRa
Shadow bytes around the buggy address:
  0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff8000: fa fa 00 00 fa fa fd fa fa fa 00 fa fa fa fd fa
  0x0c047fff8010: fa fa 04 fa fa fa fd fa fa fa 00 fa fa fa fd fa
=>0x0c047fff8020: fa fa 00[fa]fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8070: 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
==15842==ABORTING
```

poc: poc.zip

Edited 11 months ago by p870613

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

TIFFReadDirectory: fix OJPEG hack (fixes #319)

!277 ✓

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

Activity

- p870613 changed the description 11 months ago ·
- Even Rouault assigned to @rouault 11 months ago
- Even Rouault mentioned in merge request !277 (merged) 11 months ago
- Even Rouault mentioned in issue #294 (closed) 11 months ago
- Even Rouault mentioned in issue #289 (closed) 11 months ago
- Even Rouault closed via commit `87f580f3` 11 months ago
- Even Rouault closed via commit `87881e09` 11 months ago
- Even Rouault mentioned in commit `m-ab-s/libtiff@87881e09` 11 months ago
- Even Rouault mentioned in commit `m-ab-s/libtiff@87f580f3` 11 months ago

Please register or sign in to reply