Closed Issue created 9 months ago by Chintan Shah

/tools/tiffcrop.c:6866 - Heap buffer overflow in extractImageSection

Summary - (Summarize the bug encountered concisely)

There is a Heap buffer overflow in /tools/tiffcrop.c:6866 in extractImageSection function.

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.gi
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 commmand :

./tiffcrop -i -E l -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


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

- AddressSanitizer logs (ASAN)

```
TIFFReadDirectoryCheckOrder: Warning, Invalid TIFF directory; tags are not sorted in ascending order
TIFFReadDirectory: Warning, Unknown field with tag 4610 (0x1202) encountered.
TIFFReadDirectory: Warning, TIFF directory is missing required "StripByteCounts" field, calculating
LogLuvInitState: No support for converting user data format to LogLuv.
LogLuvInitState: No support for converting user data format to LogLuv.
a.tif: Error, can't write strip 0.
LogLuvInitState: No support for converting user data format to LogLuv.
```

```
a.tif: Error, can't write strip 0.
=================================================================
==14324==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x631000027403 at pc 0x5572c0c22f8
READ of size 1 at 0x631000027403 thread T0
    #0 0x5572c0c22f81 in extractImageSection /home/targets/libtiff/tools/tiffcrop.c:6866
    #1 0x5572c0c25409 in writeImageSections /home/targets/libtiff/tools/tiffcrop.c:7097
    #2 0x5572c0bf8927 in main /home/targets/libtiff/tools/tiffcrop.c:2451
    #3 0x7efc355f20b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #4 0x5572c0beadcd in _start (/home/targets/libtiff/tools/tiffcrop+0x267dcd)

0x631000027403 is located 1 bytes to the right of 76802-byte region [0x631000014800,0x631000027402)
allocated by thread T0 here:
    #0 0x7efc363a2bc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x5572c0cf5d57 in _TIFFmalloc /home/targets/libtiff/libtiff/tif_unix.c:314
    #2 0x5572c0beaf8c in limitMalloc /home/targets/libtiff/tools/tiffcrop.c:627
    #3 0x5572c0c2fabe in rotateImage /home/targets/libtiff/tools/tiffcrop.c:8479
    #4 0x5572c0c2ba64 in createCroppedImage /home/targets/libtiff/tools/tiffcrop.c:7771
    #5 0x5572c0bf82a2 in main /home/targets/libtiff/tools/tiffcrop.c:2404
    #6 0x7efc355f20b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/targets/libtiff/tools/tiffcrop.c:6866 in extra
Shadow bytes around the buggy address:
  0x0c627fffce30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c627fffce40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c627fffce50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c627fffce60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c627fffce70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c627fffce80:[02]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c627fffce90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c627fffcea0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c627fffceb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c627fffcec0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c627fffced0: 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
  Shadow gap:              cc
==14324==ABORTING
```

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

Su Laus @Su_Laus · 9 months ago Developer

The cause of the error for issue 380 is an incorrect formula in `extractImageSection()`. The whole function looks like it is still fully under development. That's why I'm not sure that correcting the formula is enough. I fear further side effects.

```
tiffcrop.c:6788
  img_rowsize = ((img_width * bps + 7) / 8) * spp;  /*ToDo: This formula is wrong and caus
  full_bytes = (sect_width * spp * bps) / 8;   /* number of COMPLETE bytes per row in sect
  trailing_bits = (sect_width * bps) % 8;       /*ToDo: This formula might also be wrong
```

I think, the right formula should be:

```
img_rowsize = ((img_width * bps * spp + 7) / 8);
trailing_bits = (sect_width * bps * spp) % 8;
```

Su Laus @Su_Laus · 9 months ago Developer

I also noticed the following code in `createCroppedImage()`:

```
tiffcrop:7684
  crop_buff = read_buff;    /*ToDo: This seams to be useless statement, because a few line
  *crop_buff_ptr = read_buff;
  crop->combined_width = image->width;
  crop->combined_length = image->length;

  cropsize = crop->bufftotal;
  crop_buff = *crop_buff_ptr;
  if (!crop_buff)
    {                   /*ToDo: This will never happen, because crop_buff is up to here se
    crop_buff = (unsigned char *)limitMalloc(cropsize);
    *crop_buff_ptr = crop_buff;
    _TIFFmemset(crop_buff, 0, cropsize);
    prev_cropsize = cropsize;
    }
  else
```

and also

```
tiffcrop:7781
  /*ToDo: Check this statement below. crop_buff is set to read_buff and the only way to ch
  if (crop_buff == read_buff) /* we used the read buffer for the crop buffer */
    *read_buff_ptr = NULL;    /* so we don't try to free it later */

  return (0);
```

Chintan Shah @shahcs · 9 months ago Author

@Su_Laus , Thanks for taking a look at this issue. I hope you were able to reproduce this with the POC attached.

- Would you like to make a fix for this and also comment on other ones : 379, 381,382 and 386 whenever you get a chance ?

Su Laus mentioned in merge request !307 (merged) 9 months ago

Chintan Shah @shahcs · 8 months ago

Author

@Su_Laus ,

I noticed that you've addressed Issue 382 as well along with this fix. Couple of questions :

- Are these 2 separate fixes for two different issues (380 and 382) ?
- It is recommended for the maintainer of the code to request a CVE from GitLab. In this case, I have already requested for them. Would you comment on the below request raised for issuing the CVE. If you think we need 2 CVEs for both these issues , please call that out as well .

https://gitlab.com/gitlab-org/cves/-/issues/367

Edited by Chintan Shah 8 months ago

Su Laus closed via commit `232282fd` 8 months ago

Even Rouault mentioned in commit `46dc8fcd` 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