Closed Issue created 8 months ago by 4ugustus

tiffcrop: SEGV in _TIFFmemset, tif_unix.c:340

Summary

There is a SEGV in _TIFFmemset in libtiff/tif_unix.c:340. 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 77 (0x4d) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 501 (0x1f5) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 11345 (0x2c51) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 18761 (0x4949) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 1536 (0x600) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 65328 (0xff30) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 63231 (0xf6ff) encountered.
TIFFFetchNormalTag: Warning, Incorrect count for "NumberOfInks"; tag ignored.
TIFFFetchNormalTag: Warning, Incorrect count for "Orientation"; tag ignored.
TIFFFetchNormalTag: Warning, ASCII value for tag "PageName" does not end in null byte.
TIFFAdvanceDirectory: Error fetching directory link.
loadImage: Image lacks Photometric interpretation tag.
Fax4Decode: Warning, Line length mismatch at line 0 of strip 0 (got 133, expected 132).
Fax4Decode: Warning, Premature EOL at line 2 of strip 0 (got 20, expected 132).
MemoryLimitError: allocation of 271321920 bytes is forbidden. Limit is 268435456.
                  use -k option to change limit.
ASAN:DEADLYSIGNAL
=================================================================
==3830458==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f1b9e7efe6d bp 0x7
==3830458==The signal is caused by a WRITE memory access.
==3830458==Hint: address points to the zero page.
    #0 0x7f1b9e7efe6c  (/lib/x86_64-linux-gnu/libc.so.6+0x18ee6c)
    #1 0x7f1b9f707cde  (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x5ecde)
    #2 0x5614b85ff803 in _TIFFmemset /root/programs/libtiff/libtiff/tif_unix.c:340
    #3 0x5614b8588197 in createImageSection /root/programs/libtiff/tools/tiffcrop.c:7410
    #4 0x5614b8586c05 in writeImageSections /root/programs/libtiff/tools/tiffcrop.c:7096
    #5 0x5614b856ce78 in main /root/programs/libtiff/tools/tiffcrop.c:2451
    #6 0x7f1b9e682bf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
    #7 0x5614b8563869 in _start (/root/programs/libtiff/build_asan/bin/tiffcrop+0x28869)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/lib/x86_64-linux-gnu/libc.so.6+0x18ee6c)
==3830458==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 3

fix the SEGV in tiffcrop

!308

fix the FPE in tiffcrop (#393)

!310

add checks for return value of limitMalloc (#392)

!314

When these merge requests are accepted, this issue will be closed automatically.

Activity

4ugustus @waugustus · 8 months ago

Author Contributor

Analysis

Crash Cause

With gdb, we can print the backtrace as follows.

```
gdb-peda$ bt
#0  __memset_avx2_erms () at ../sysdeps/x86_64/multiarch/memset-vec-unaligned-erms.S:151
#1  0x000055555559a253 in _TIFFmemset (p=0x0, v=0x0, c=0x1093fb60) at tif_unix.c:340
#2  0x000055555556c100 in createImageSection (sectsize=0x1093fb60, sect_buff_ptr=0x7fffff
#3  0x000055555556b3f5 in writeImageSections (in=0x555555617eb0, out=0x55555561ac60, image
    src_buff=0x7fffe7daf010 "", sect_buff_ptr=0x7fffffff8ed8) at tiffcrop.c:7096
#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 ()
```

It is weird that the pointer *p* is a NULL pointer. From code, we can find that the NULL pointer is from createImageSection, tiffcrop.c:7408.

```
sect_buff = (unsigned char *)limitMalloc(sectsize);
*sect_buff_ptr = sect_buff;
_TIFFmemset(sect_buff, 0, sectsize);
```

The *sectsize* is equal to 0x0x1093fb60 here, which is greater than maxMalloc in limitMalloc, tiffcrop.c:620

```
static void* limitMalloc(tmsize_t s)
{
  if (maxMalloc && (s > maxMalloc)) {
    fprintf(stderr, "MemoryLimitError: allocation of %" PRIu64 " bytes is forbidden. Limit
            (uint64_t)s, (uint64_t)maxMalloc);
    fprintf(stderr, "                  use -k option to change limit.\n");
    return NULL;
  }
  return _TIFFmalloc(s);
}
```

Since the function createImageSection does not check the return value, the program crashes.

How to fix

Add checks before _TIFFmemset as follows.

```
sect_buff = (unsigned char *)limitMalloc(sectsize);
*sect_buff_ptr = sect_buff;

if (!sect_buff)
{
    TIFFError("createImageSection", "Unable to allocate/reallocate section buffer");
    return (-1);
}

_TIFFmemset(sect_buff, 0, sectsize);
```

Note that, there are some similar bugs in tiffcrop.c:7420, tiffcrop.c:7699, and tiffcrop.c:7716. We can use the same way to fix them, as shown in !314 (merged)

Edited by 4ugustus 8 months ago

4ugustus mentioned in merge request !308 (closed) 8 months ago

4ugustus mentioned in merge request !310 (merged) 8 months ago

4ugustus mentioned in merge request !314 (merged) 8 months ago

4ugustus mentioned in commit `40b00cfb` 8 months ago

Even Rouault mentioned in commit `f2b656e2` 8 months ago

Even Rouault closed via merge request !314 (merged) 8 months ago

Please register or sign in to reply