Closed Issue created 7 months ago by 4ugustus

tiffcp: SEGV in LZWDecode, tif_lzw.c:619 and tif_lzw.c:624

Summary

There is SEGV errors in LZWDecode in libtiff/tif_lzw.c:619 and libtiff/tif_lzw.c:624. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted tiff file.

Version

LIBTIFF, Version master (post 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/tiffcp -i poc1 /tmp/foo
TIFFReadDirectoryCheckOrder: Warning, Invalid TIFF directory; tags are not sorted in ascending order
TIFFReadDirectory: Warning, Unknown field with tag 0 (0x0) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 32512 (0x7f00) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 45521 (0xb1d1) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 513 (0x201) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 771 (0x303) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 53456 (0xd0d0) encountered.
TIFFFetchNormalTag: Warning, Incorrect count for "PhotometricInterpretation"; tag ignored.
TIFFFetchNormalTag: Warning, IO error during reading of "DocumentName"; tag ignored.
_TIFFVSetField: output_tiffcp_random_3/default/crashes/id:000000,sig:11,src:003319,time:155007069,ex
LZWDecode: Not enough data at scanline 0 (short 2018 bytes).
output_tiffcp_random_3/default/crashes/id:000000,sig:11,src:003319,time:155007069,execs:29344422,op:
ASAN:DEADLYSIGNAL
=================================================================
==1076584==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000000b (pc 0x55ac4b6f03c6 bp 0x7
==1076584==The signal is caused by a READ memory access.
==1076584==Hint: address points to the zero page.
    #0 0x55ac4b6f03c5 in LZWDecode /root/programs/libtiff/libtiff/tif_lzw.c:619
    #1 0x55ac4b726b20 in TIFFReadScanline /root/programs/libtiff/libtiff/tif_read.c:447
    #2 0x55ac4b64a607 in cpContig2ContigByRow /root/programs/libtiff/tools/tiffcp.c:1014
    #3 0x55ac4b64a470 in tiffcp /root/programs/libtiff/tools/tiffcp.c:979
    #4 0x55ac4b6472d5 in main /root/programs/libtiff/tools/tiffcp.c:334
    #5 0x7ff15d37cc86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #6 0x55ac4b645db9 in _start (/root/programs/libtiff/build_asan/bin/tiffcp+0x26db9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /root/programs/libtiff/libtiff/tif_lzw.c:619 in LZWDecode
==1076584==ABORTING
```

```
./build_asan/bin/tiffcp -i poc2 /tmp/foo
TIFFReadDirectoryCheckOrder: Warning, Invalid TIFF directory; tags are not sorted in ascending order
TIFFReadDirectory: Warning, Unknown field with tag 0 (0x0) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 63242 (0xf70a) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 18688 (0x4900) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 45521 (0xb1d1) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 51721 (0xca09) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 513 (0x201) encountered.
TIFFReadDirectory: Warning, Unknown field with tag 1023 (0x3ff) encountered.
TIFFFetchNormalTag: Warning, Incorrect count for "PhotometricInterpretation"; tag ignored.
TIFFFetchNormalTag: Warning, ASCII value for tag "Tag 63242" does not end in null byte. Forcing it t
TIFFFetchNormalTag: Warning, IO error during reading of "DocumentName"; tag ignored.
_TIFFVSetField: output_tiffcp_random_3/default/crashes/id:000011,sig:11,src:005277,time:304660840,ex
LZWDecode: Not enough data at scanline 0 (short 121315 bytes).
output_tiffcp_random_3/default/crashes/id:000011,sig:11,src:005277,time:304660840,execs:63494869,op:
ASAN:DEADLYSIGNAL
=================================================================
==475857==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000000b (pc 0x55a0bf7f7483 bp 0x7f
==475857==The signal is caused by a READ memory access.
```

```
==475857==Hint: address points to the zero page.
    #0 0x55a0bf7f7482 in LZWDecode /root/programs/libtiff/libtiff/tif_lzw.c:624
    #1 0x55a0bf82db20 in TIFFReadScanline /root/programs/libtiff/libtiff/tif_read.c:447
    #2 0x55a0bf751607 in cpContig2ContigByRow /root/programs/libtiff/tools/tiffcp.c:1014
    #3 0x55a0bf751470 in tiffcp /root/programs/libtiff/tools/tiffcp.c:979
    #4 0x55a0bf74e2d5 in main /root/programs/libtiff/tools/tiffcp.c:334
    #5 0x7f5badb6cc86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #6 0x55a0bf74cdb9 in _start (/root/programs/libtiff/build_asan/bin/tiffcp+0x26db9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /root/programs/libtiff/libtiff/tif_lzw.c:624 in LZWDecode
==475857==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
```

poc1 poc2

Edited 7 months ago by Even Rouault

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.

Activity

Even Rouault changed the description 7 months ago ·

Even Rouault @rouault · 7 months ago Owner

master only issue due 3079627e

Even Rouault closed via commit b4e79bfa 7 months ago

Even Rouault @rouault · 7 months ago Owner

fixed per b4e79bfa

Even Rouault mentioned in commit freedesktop-sdk/mirrors/gitlab/libtiff/libtiff@b4e79bfa 7 months ago

Even Rouault mentioned in commit sanrep/docker-gdal@d8c1073e 7 months ago

Petter Reinholdtsen @petterreinholdtsen · 5 months ago

For the record, this is https://security-tracker.debian.org/tracker/CVE-2022-1622 .

Please register or sign in to reply