Closed Issue created 9 months ago by **Chintan Shah**

AddressSanitizer: undefined-behavior tif_dirread.c:4176:40 in TIFFReadDirectory function

Summary

Null pointer passed as an argument to memcpy in TIFFReadDirectory function in tools/tif_dirread.c:4176:40 resulting into Denial of Service when crafted TIFF image is parsed by library

(libtiff version) libtiff version 4.3.0 downloaded from https://download.osgeo.org/libtiff/tiff-4.3.0.zip

Steps to reproduce

tiff 4.3.0.zip downloaded from https://download.osgeo.org/libtiff/tiff-4.3.0.zip

compile the library with the AFL compiler wrapper using LLVM instrumentation and with ASAN and UBSAN enabled as shown below:

CC=afl-clang-fast CXX=afl-clang-fast++ CFLAGS="-g -fsanitize=address,undefined -fno-sanitize-recover=all" CXXFLAGS="-g -fsanitize=address,undefined -fno-sanitize-recover=all" LDFLAGS="-fsanitize=address,undefined -fno-sanitize-recover=all -lm" ./configure --disable-shared

OR

CC=gcc CXX=g++ CFLAGS="-g -fsanitize=address,undefined -fno-sanitize-recover=all" CXXFLAGS="-g -fsanitize=address,undefined -fno-sanitize-recover=all" LDFLAGS="-fsanitize=address,undefined -fno-sanitize-recover=all -lm" ./configure --disable-shared

execute the tiffinfo binary with the following options and the crafted TIFF POC image: ./tiffinfo -f lsb2msb -Dcdjrsz crash.tif

TIFFReadDirectoryCheckOrder: Warning, Invalid TIFF directory; tags are not sorted in ascending order.

TIFFReadDirectory: Warning, Unknown field with tag 18770 (0x4952) encountered.

TIFFFetchNormalTag: Warning, Incorrect count for "PhotometricInterpretation"; tag ignored.

TIFFFetchNormalTag: Warning, Incorrect value for "DateTime"; tag ignored.

TIFFReadDirectory: Warning, Sum of Photometric type-related color channels and ExtraSamples doesn't match

SamplesPerPixel. Defining non-color channels as ExtraSamples..

tif_dirread.c:4176:40: runtime error: null pointer passed as argument 2, which is declared to never be null
/usr/include/string.h:43:28: note: nonnull attribute specified here

SUMMARY: AddressSanitizer: undefined-behavior tif_dirread.c:4176:40

```
 memcpy(new_sampleinfo, tif->tif_dir.td_sampleinfo, old_extrasamples * sizeof(uint16_t));
_TIFFsetShortArray(&tif->tif_dir.td_sampleinfo, new_sampleinfo, tif>tif_dir.td_extrasamples);
_TIFFfree(new_sampleinfo);
```

Debugging Information and POC file attached

crash.zip

Platform

(Operating system, architecture, compiler details) Ubuntu 20.4 LTS 64 bit compiler used : afl-clang-fast and afl-clang-fast++ with ASAN and UBSAN enabled with the compilation command as shown above.

Edited 9 months ago by Chintan Shah

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

Chintan Shah changed the description 9 months ago ·

Chintan Shah changed the description 9 months ago ·

Even Rouault closed via commit 561599c9 9 months ago

Even Rouault mentioned in commit gitlab-org/build/omnibus-mirror/libtiff@561599c9 9 months ago

Chintan Shah @shahcs · 9 months ago Author

Hi @rouault

There is one more potential issue similar to the one you've patched. This is in tif_unix.c

---

Here is the output from the crash file. Reproduction steps remains the same. POC file attached.

TIFFReadDirectoryCheckOrder: Warning, Invalid TIFF directory; tags are not sorted in ascending order.

TIFFReadDirectory: Warning, Unknown field with tag 1024 (0x400) encountered.

TIFFReadDirectory: Warning, Unknown field with tag 1280 (0x500) encountered.

TIFFReadDirectory: Warning, Unknown field with tag 768 (0x300) encountered.

TIFFReadDirectory: Warning, Unknown field with tag 512 (0x200) encountered.

TIFFReadDirectory: Warning, Unknown field with tag 519 (0x207) encountered.

TIFFReadDirectory: Warning, Unknown field with tag 520 (0x208) encountered.

TIFFReadDirectory: Warning, Unknown field with tag 521 (0x209) encountered. TIFFFetchNormalTag: Warning, Incorrect value for "Model"; tag ignored.

TIFFReadDirectory: Warning, SamplesPerPixel tag is missing, applying correct SamplesPerPixel value of 3. TIFFFetchStripThing: Warning, Incorrect count for "StripOffsets"; tag ignored.

tif_unix.c:346:2: runtime error: null pointer passed as argument 2, which is declared to never be null

---

crash2.tif

Chintan Shah reopened 9 months ago

Even Rouault closed via commit `eecb0712` 9 months ago

Even Rouault @rouault · 9 months ago — Owner

Fix for crash2.tif committed in `eecb0712`

Even Rouault mentioned in commit `freedesktop-sdk/mirrors/gitlab/libtiff/libtiff@eecb0712` 9 months ago

Chintan Shah @shahcs · 9 months ago — Author

Also @rouault , do you see the need for ? assigning a CVE for both these issues ?

Even Rouault @rouault · 9 months ago — Owner

Personally I'm staying out of CVE business. If others want to deal with that, they're free to do so.

Timothy Lyanguzov @theta682 · 9 months ago — Contributor

This issue has assigned CVE-2022-0561 and CVE-2022-0562. @bobfriesenhahn can you make a release with this fix?

Ozkan Sezer mentioned in commit `freedesktop-sdk/mirrors/github/libsdl-org/SDL_image@19a9b461` 6 months ago