

# AddressSanitizer: Null Pointer Dereference in tif\_unix.c:346

## Summary

`std::memcpy` is being called when `const void* src` is `NULL`. In this case, it's `s=0x0` according to `TIFFmemcpy` (`d=0x85a750`, `s=0x0`, `c=0`) at `tif_unix.c:346`. In `tif_dirread.c:5094`, it calls `_TIFFmemcpy(o,data,(uint32_t)dp->tdir_count)` without checking the variable `data`.

```
(gdb) frame 1
#1 0x000000000482f8e in TIFFFetchNormalTag (tif=0x859e90, dp=0x85a550, recover=1) at tif_dirread.c:5094
(gdb) list 5090
5085             o=NULL;
5086         else
5087             o=_TIFFmalloc((uint32_t)dp->tdir_count);
5088         if (o==NULL)
5089         {
5090             if (data!=NULL)
5091                 _TIFFfree(data);
5092             return(0);
5093         }
5094         _TIFFmemcpy(o,data,(uint32_t)dp->tdir_count);
(gdb) p data
$1 = (uint8_t *) 0x0
```

Maybe a check like `if(o==NULL || data==NULL)` can be added in line 5088?

## Version

libtiff 4.3.0 (commit [180882b4](#))

## Steps to reproduce

1. `./configure CC=clang-12 CXX=clang++-12 CFLAGS="-g -fsanitize=undefined -fsanitize=undefined-trap-on-error -fno-sanitize-recover=all -fno-omit-frame-pointer -Wall -W" --disable-shared` compile
2. `gdb tiff2pdf`
3. `(gdb) set args POC`
4. `(gdb) r`

 [POC](#)

## Backtrace


```
Program received signal SIGILL, Illegal instruction.
0x0000000006130a9 in _TIFFmemcpy (d=0x85a750, s=0x0, c=0) at tif_unix.c:346
346             memcpy(d, s, (size_t) c);
(gdb) bt
#0 0x0000000006130a9 in _TIFFmemcpy (d=0x85a750, s=0x0, c=0) at tif_unix.c:346
#1 0x000000000482f8e in TIFFFetchNormalTag (tif=0x859e90, dp=0x85a550, recover=1) at tif_dirread.c:5094
#2 0x0000000004798c0 in TIFFReadDirectory (tif=0x859e90) at tif_dirread.c:3996
#3 0x0000000005b78b9 in TIFFClientOpen (name=0x7fffffff648 "POC", mode=0x625070 "r", clientdata=0, closeproc=0x612b00 <_tiffCloseProc>, sizeproc=0x612b30 <_tiffSizeProc>, mapproc=0x612be0 <_tiffMapProc>) at tif_unix.c:248
#4 0x0000000006126d4 in TIFFFdOpen (fd=3, name=0x7fffffff648 "POC", mode=0x625070 "r") at tif_unix.c:248
#5 0x000000000612eeb in TIFFOpen (name=0x7fffffff648 "POC", mode=0x625070 "r") at tif_unix.c:248
#6 0x0000000004040d9 in main (argc=2, argv=0x7fffffff388) at tiff2pdf.c:766
```

## Platform

18.04.1-Ubuntu x86\_64 GNU/Linux

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 closed via commit [a95b799f](#) 9 months ago



Even Rouault mentioned in commit [gitlab-org/build/omnibus-mirror/libtiff@a95b799f](#) 9 months ago



Ozkan Sezer mentioned in commit [freedesktop-sdk/mirrors/github/libSDL-org/SDL\\_image@19a9b461](#) 6 months ago

Please [register](#) or [sign in](#) to reply