AddressSanitizer: stack-buffer-overflow /home/lin/Downloads/libtiff/tools/tiffcp.c:289 in main

AddressSanitizer: stack-buffer-overflow /home/lin/Downloads/libtiff/tools/tiffcp.c:289 in main

Version

```
→ tiffcp_test2 ./tiffcp -v
./tiffcp: invalid option -- 'v'
LIBTIFF, Version 4.3.0
Copyright (c) 1988-1996 Sam Leffler
Copyright (c) 1991-1996 Silicon Graphics, Inc.
```

At branch 5e180045 (libtiff version)

Steps to reproduce

```
git clone git@gitlab.com:libtiff/libtiff.git
cd libtiff/
./autogen.sh
./configure CC=gcc CXX=g++ CFLAGS="-g -fsanitize=address" --disable-shared & make
./tools/tiffcp -8 -8 -8 -8 -8 -8 -8 -8 -8 -8 ./i ./i
```

(How one can reproduce the issue - this is very important)

Platform

```
→ libtiff git:(master) X gcc --version
gcc (Ubuntu 7.5.0-3ubuntu1~18.04) 7.5.0
Copyright (C) 2017 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.

→ libtiff git:(master) X uname -r
5.4.0-91-generic
→ libtiff git:(master) X lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description: Ubuntu 18.04.5 LTS
Release: 18.04
Codename: bionic
```

(Operating system, architecture, compiler details)

ASAN

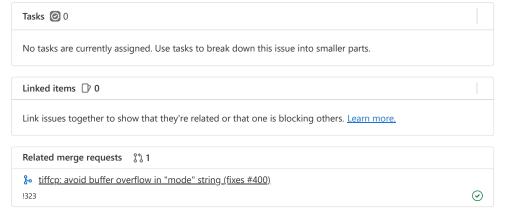
```
→ libtiff git:(Fix_Issue#330) X ./tools/tiffcp -8 -8 -8 -8 -8 -8 -8 -8 -8 -8 ./i ./i
______
==32123==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffe708226ea at pc 0x5571a24c4b
WRITE of size 1 at 0x7ffe708226ea thread T0
   #0 0x5571a24c4be7 in main /home/lin/Downloads/libtiff/tools/tiffcp.c:289
   #1 0x7f65ba8d5c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
   #2 0x5571a24c3a49 in _start (/home/lin/Downloads/libtiff/tools/tiffcp+0x23a49)
Address 0x7ffe708226ea is located in stack of thread TO at offset 170 in frame
   #0 0x5571a24c4107 in main /home/lin/Downloads/libtiff/tools/tiffcp.c:181
 This frame has 3 object(s):
   [32, 34) 'samples'
   [96, 104) 'imageCursor'
   [160, 170) 'mode' <== Memory access at offset 170 overflows this variable
HINT: this may be a false positive if your program uses some custom stack unwind mechanism or swapco
     (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow /home/lin/Downloads/libtiff/tools/tiffcp.c:289 in m
Shadow bytes around the buggy address:
```

```
0x10004e0fc4c0: 00 00 00 00 00 00 00 f1 f1 f1 f1 f2 f2 f2
=>0x10004e0fc4d0: f2 f2 f2 f2 00 f2 f2 f2 f2 f2 f2 f2 00[02]f2 f2
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable:
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:
            fa
Freed heap region:
Stack left redzone: f1
Stack mid redzone:
Stack right redzone: f3
Stack after return:
Stack use after scope: f8
Global redzone:
Global init order: f6
Poisoned by user:
Container overflow: fc
Array cookie:
Intra object redzone: bb
ASan internal:
Left alloca redzone: ca
Right alloca redzone: cb
==32123==ABORTING
```

Because it's a command line argument problem, there is no poc.

Thanks !!

1 Drag your designs here or click to upload.



When this merge request is accepted, this issue will be closed automatically.

Activity

(F)	<u>Su Laus</u> mentioned in merge request <u>!323 (merged)</u> 7 months ago
(P)	Even Rouault mentioned in commit 9752dae8 7 months ago
Θ	Even Rouault_closed via merge request <u>!324 (merged)</u> 7 months ago
(P)	Even Rouault mentioned in commit clae29f9 6 months ago
	Su Laus mentioned in commit gitlab-org/build/omnibus-mirror/libtiff@fb1db384 6 months ago

Please <u>register</u> or <u>sign in</u> to reply