CVE-2016-10268

描述：tools/tiffcp.c in LibTIFF 4.0.7 allows remote attackers to cause a denial of service (integer underflow and heap-based buffer under-read) or possibly have unspecified other impact via a crafted TIFF image, related to "READ of size 78490" and libtiff/tif\_unix.c:115:23.

软件：LibTIFF 4.0.7

源码： tools/tiffcp.c libtiff/tif\_unix.c

出现位置： tools/tiffcp.c：985-991行 libtiff/tif\_unix.c：109-118行

关键源码：

tools/tiffcp.c：

tstrip\_t s, ns = TIFFNumberOfStrips(in);

uint32 row = 0;

\_TIFFmemset(buf, 0, stripsize);

- for (s = 0; s < ns; s++) {

+ for (s = 0; s < ns && row < imagelength; s++) {

tsize\_t cc = (row + rowsperstrip > imagelength) ?

TIFFVStripSize(in, imagelength - row) : stripsize;

if (TIFFReadEncodedStrip(in, s, buf, cc) < 0

libtiff/tif\_unix.c：

for (bytes\_written=0; bytes\_written < bytes\_total; bytes\_written+=count)

{

const char \*buf\_offset = (char \*) buf+bytes\_written;

size\_t io\_size = bytes\_total-bytes\_written;

if (io\_size > TIFF\_IO\_MAX)

io\_size = TIFF\_IO\_MAX;

count=write(fdh.fd, buf\_offset, (TIFFIOSize\_t) io\_size);

if (count <= 0)

break;

}