CVE-2016-10272

描述：LibTIFF 4.0.7 allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted TIFF image, related to "WRITE of size 2048" and libtiff/tif\_next.c:64:9.

软件：LibTIFF 4.0.7

源码：tiffcrop.c tif\_next.c

出现位置： tiffcrop.c：3688-3702行 tif\_next.c：63-64行

关键源码：

Tiffcrop.c:

for (strip = 0; strip < nstrips; strip++) {

bytes\_read = TIFFReadEncodedStrip (in, strip, bufp, -1);

rows = bytes\_read / scanline\_size;

if ((strip < (nstrips - 1)) && (bytes\_read != (int32)stripsize))

TIFFError("", "Strip %d: read %lu bytes, strip size %lu",

(int)strip + 1, (unsigned long) bytes\_read,

(unsigned long)stripsize);

if (bytes\_read < 0 && !ignore) {

TIFFError("", "Error reading strip %lu after %lu rows",

(unsigned long) strip, (unsigned long)rows);

return 0;

}

bufp += bytes\_read;

}

tif\_next.c:

for (op = (unsigned char\*) buf, cc = occ; cc-- > 0;)

\*op++ = 0xff;