CVE-2016-10270

描述：LibTIFF 4.0.7 allows remote attackers to cause a denial of service (heap-based buffer over-read) or possibly have unspecified other impact via a crafted TIFF image, related to "READ of size 8" and libtiff/tif\_read.c:523:22.

软件：LibTIFF 4.0.7

源码： libtiff/tif\_read.c

出现位置： 5539-5572行

关键源码：

if (rowsperstrip >= td->td\_rowsperstrip)

return;

nstrips64 = TIFFhowmany\_64(bytecount, stripbytes);

if ((nstrips64==0)||(nstrips64>0xFFFFFFFF)) /\* something is wonky, do nothing. \*/

return;

nstrips32 = (uint32)nstrips64;

newcounts = (uint64\*) \_TIFFCheckMalloc(tif, nstrips32, sizeof (uint64),

"for chopped \"StripByteCounts\" array");

newoffsets = (uint64\*) \_TIFFCheckMalloc(tif, nstrips32, sizeof (uint64),

"for chopped \"StripOffsets\" array");

if (newcounts == NULL || newoffsets == NULL) {

/\*

\* Unable to allocate new strip information, give up and use

\* the original one strip information.

\*/

if (newcounts != NULL)

\_TIFFfree(newcounts);

if (newoffsets != NULL)

\_TIFFfree(newoffsets);

return;

}

/\*

\* Fill the strip information arrays with new bytecounts and offsets

\* that reflect the broken-up format.

\*/

循环复制

for (strip = 0; strip < nstrips32; strip++) {

if (stripbytes > bytecount)

stripbytes = bytecount;

newcounts[strip] = stripbytes;

newoffsets[strip] = offset;

offset += stripbytes;

bytecount -= stripbytes;

}