CVE-2016-10094

描述：Off-by-one error in the t2p\_readwrite\_pdf\_image\_tile function in tools/tiff2pdf.c in LibTIFF 4.0.7 allows remote attackers to have unspecified impact via a crafted image.

软件：LibTIFF 4.0.7

源码：libtiff/tif\_unix.c

出现位置：115 行

关键源码：

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); //overflow

if (count <= 0)

break;

}