CVE-2016-10095

描述：Stack-based buffer overflow in the \_TIFFVGetField function in tif\_dir.c in LibTIFF 4.0.7 allows remote attackers to cause a denial of service (crash) via a crafted TIFF file.

软件：LibTIFF 4.0.7

源码：libtiff/tif\_dir.c

出现位置： 1077行

关键源码：

if (fip->field\_passcount) {

if (fip->field\_readcount == TIFF\_VARIABLE2)

\*va\_arg(ap, uint32\*) = (uint32)tv->count;

else /\* Assume TIFF\_VARIABLE \*/

\*va\_arg(ap, uint16\*) = (uint16)tv->count;

\*va\_arg(ap, void \*\*) = tv->value;

ret\_val = 1;