CVE-2017-6852

描述：Heap-based buffer overflow in the jpc\_dec\_decodepkt function in jpc\_t2dec.c in JasPer 2.0.10 allows remote attackers to have unspecified impact via a crafted image.

软件：JasPer 2.0.10

源码：src/libjasper/jpc/jpc\_t2dec

出现位置： 239-247行

关键源码：

for (bandno = 0, band = rlvl->bands; bandno < rlvl->numbands;

++bandno, ++band) {

if (!band->data) {

continue;

}

prc = &band->prcs[prcno];

if (!prc->cblks) {

continue;

}