CVE-2016-10249

描述：Integer overflow in the jpc\_dec\_tiledecode function in jpc\_dec.c in JasPer before 1.900.12 allows remote attackers to have unspecified impact via a crafted image file, which triggers a heap-based buffer overflow.

软件：JasPer 1.900.10

源码：src/libjasper/jpc/jpc\_dec.c

出现位置： 1101-1109行

关键源码：

循环复制：

for (compno = 0, tcomp = tile->tcomps, cmpt = dec->cmpts; compno <

dec->numcomps; ++compno, ++tcomp, ++cmpt) {

adjust = cmpt->sgnd ? 0 : (1 << (cmpt->prec - 1));

for (i = 0; i < jas\_matrix\_numrows(tcomp->data); ++i) {

for (j = 0; j < jas\_matrix\_numcols(tcomp->data); ++j) {

\*jas\_matrix\_getref(tcomp->data, i, j) += adjust;

}

}

}