CVE-2017-7870

描述： LibreOffice before 2017-01-02 has an out-of-bounds write caused by a heap-based buffer overflow related to the tools::Polygon::Insert function in tools/source/generic/poly.cxx.

软件： LibreOffice

源码： tools/source/generic/poly.cxx

出现位置： 224-237行

关键源码：

if( nPos >= mnPoints )

{

// Append at the back

nPos = mnPoints;

ImplSetSize( nNewSize );

if( pInitPoly )

{

memcpy( mpPointAry + nPos, pInitPoly->mpPointAry, nSpaceSize );

if( pInitPoly->mpFlagAry )

memcpy( mpFlagAry + nPos, pInitPoly->mpFlagAry, nSpace );

}

}