CVE-2017-7856

描述：LibreOffice before 2017-03-11 has an out-of-bounds write caused by a heap-based buffer overflow in the SVMConverter::ImplConvertFromSVM1 function in vcl/source/gdi/svmconverter.cxx.

软件：LibreOffice

源码：vcl/source/gdi/svmconverter.cxx.

出现位置： 988-994行

关键源码：

数组越界

if( nStrLen > 1 )

pDXAry[ nStrLen-3 ] = pDXAry[ nStrLen-2 ] + pTmpAry[ nStrLen-1 ] - pTmpAry[ nStrLen-2 ];

else

pDXAry[ nStrLen-1 ] = pTmpAry[ nStrLen-1 ]; // len=1: 0th position taken to be 0

}