CVE-2016-10327

描述：LibreOffice before 2016-12-22 has an out-of-bounds write caused by a heap-based buffer overflow related to the EnhWMFReader::ReadEnhWMF function in vcl/source/filter/wmf/enhwmf.cxx.

软件：LibreOffice

源码：vcl/source/filter/wmf/enhwmf.cxx

出现位置： 1254-1278行

关键源码：

const sal\_uInt32 nSourceSize = cbBmiSrc + cbBitsSrc + 14;

if ( nSourceSize <= ( nEndPos - nStartPos ) )

{

// we need to read alpha channel data if AlphaFormat of BLENDFUNCTION is

// AC\_SRC\_ALPHA (==0x01). To read it, create a temp DIB-File which is ready

// for DIB-5 format

const bool bReadAlpha(0x01 == aFunc.aAlphaFormat);

const sal\_uInt32 nDeltaToDIB5HeaderSize(bReadAlpha ? getDIBV5HeaderSize() - cbBmiSrc : 0);

const sal\_uInt32 nTargetSize(cbBmiSrc + nDeltaToDIB5HeaderSize + cbBitsSrc + 14);

char\* pBuf = new char[ nTargetSize ];

SvMemoryStream aTmp( pBuf, nTargetSize, StreamMode::READ | StreamMode::WRITE );

aTmp.ObjectOwnsMemory( true );

// write BM-Header (14 bytes)

aTmp.WriteUChar( 'B' )

.WriteUChar( 'M' )

.WriteUInt32( cbBitsSrc )

.WriteUInt16( 0 )

.WriteUInt16( 0 )

.WriteUInt32( cbBmiSrc + nDeltaToDIB5HeaderSize + 14 );

// copy DIBInfoHeader from source (cbBmiSrc bytes)

pWMF->Seek( nStart + offBmiSrc );

pWMF->ReadBytes(pBuf + 14, cbBmiSrc);