CVE-2017-8378

描述：Heap-based buffer overflow in the PdfParser::ReadObjects function in base/PdfParser.cpp in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via vectors related to m\_offsets.size.

软件：PoDoFo 0.9.5

源码：/podofo-0.9.5/src/base/PdfParser.cpp

出现位置： 951-974行

关键源码：

数组越界

if( pEncrypt->IsReference() )

{

i = pEncrypt->GetReference().ObjectNumber();

pObject = new PdfParserObject( m\_vecObjects, m\_device, m\_buffer, m\_offsets[i].lOffset );

if( !pObject )

PODOFO\_RAISE\_ERROR( ePdfError\_OutOfMemory );

pObject->SetLoadOnDemand( false ); // Never load this on demand, as we will use it immediately

try {

pObject->ParseFile( NULL ); // The encryption dictionary is not encrypted :)

// Never add the encryption dictionary to m\_vecObjects

// we create a new one, if we need it for writing

// m\_vecObjects->push\_back( pObject );

m\_offsets[i].bParsed = false; //no checking its boundary

m\_pEncrypt = PdfEncrypt::CreatePdfEncrypt( pObject );

delete pObject;

} catch( PdfError & e ) {

std::ostringstream oss;

oss << "Error while loading object " << pObject->Reference().ObjectNumber() << " "

<< pObject->Reference().GenerationNumber() << std::endl;

delete pObject;

e.AddToCallstack( \_\_FILE\_\_, \_\_LINE\_\_, oss.str().c\_str() );

throw e;