

概要

Apache POI 是一个对Microsoft Office系列文档进行解析的java类库，其3.13版本及以下在2016年8月被爆出在解析Office openXML文档结构时，存在XML外部实体注入漏洞，漏洞编号cve-2016-5000。虽然漏洞披露信息中没有提及具体的漏洞利用方式，但提到了官方案例XLSX2CSV。因此，

构造payload文件

在payload文件的构造上，需要安利一个小工具oxml_xxe，具体安装配置过程不再赘述：

https://github.com/BufaloWill/oxml_xxe

首先，以XLSX文件为例，可以通过将后缀修改为zip进行解压缩，解压后的目录结构如下：

可以通过搭建的oxml_xxe工具替换其中任意xml的内容，测试是否能够触发XML外部实体注入攻击。例如，将xl/workbook.xml中的内容替换。

通过不断尝试替换各个xml文件，发现将xl/wroksheets/sheet1.xml替换为payload，可以成功触发漏洞。

漏洞重现

为配合利用XXE漏洞实现文件读取，在本地创建了一个文件/Users/sanwenkit/readme.txt，接下来将尝试利用Apache POI官方的poi-examples-3.13-20150929.jar解析构造的恶意xlsx文档payload，对文件内容进行读取，并通过dnslog（cloudeye）获取文件内容发送至远端服务器。

Apache POI官方的poi-examples-3.13-20150929.jar需要通过一些配置实现正常运行解析文件。

第一步需要下载依赖的jar包xmlbeans-2.4.0.jar、xmlbeans-xpath-2.4.0.jar，放入poi相关jar包相同目录

第二步需要对poi-examples-3.13-20150929.jar包的MANIFEST.MF进行更新，指定Main-class和Class-path。相关MANIFEST.MF文件内容如下：

```
Manifest-Version: 1.0

Ant-Version: Apache Ant 1.9.4

Created-By: 1.6.0_45-b06 (Sun Microsystems Inc.)

Built-By: andreas.beeker

Specification-Title: Apache POI

Specification-Version: 3.13

Specification-Vendor: The Apache Software Foundation

Implementation-Title: Apache POI

Implementation-Version: 3.13s

Implementation-Vendor-Id: org.apache.poi

Implementation-Vendor: The Apache Software Foundation

Main-Class: org.apache.poi.xssf.eventusermodel.XLSX2CSV

Class-Path: poi-3.13-20150929.jar poi-ooxml-3.13-20150929.jar poi-ooxml-schemas-3.13-20150929.jar poi-excelant-3.13-20150929.jar
```

更新jar包的命令为：

```
jar umf PATH_TO_MANIFEST poi-examples-3.13-20150929.jar
```

完成所有准备后，执行Apache POI示例程序程序对生成的恶意xlsx文档进行解析：

```
java -jar poi-examples-3.13-20150929.jar PATH_TO_PAYLOAD
```

解析结果如下图所示：

可以看到已经触发了漏洞，Apache POI将readme.txt文档中的内容“poi-xxe-demo”发送到了接收URL地址：



[0c0c0f](#) 2017-01-10 13:04:26

赞 应用的具体攻击入口有吗？

0 回复Ta



[sanwenkit](#) 2017-01-11 07:51:08

并没有特意去看哪些开源代码调用了这个类库，平时碰到office文件的上传点可以用构造的恶意文件盲打试试。也请师傅们多指教姿势~

0 回复Ta

[登录](#) 后跟帖
 先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#)
[关于社区](#)
[友情链接](#)
[社区小黑板](#)