登录

Apache FOP-XXE—【CVE-2017-5661】

orich1 / 2018-01-15 09:32:00 / 浏览数 2856 技术文章 技术文章 顶(0) 踩(0)

Apache FOP

FOP (Formatting Objects Processor) 是第一个基于 XSL:FO
的打印格式处理器，也是第一个与输出无关的格式处理器。能够从对象树中读入，然后生成渲染过的页面，将其输出到指定的流。目前支持的输出格式有PDF,PCL,PS,SVG,X

漏洞简介

Fixed in FOP 2.2
medium: XXE vulnerability CVE-2017-5661
Issue Public: 2017-04-18
Update Released: 2017-04-10 (FOP 2.2)
Affects: 2.1 and earlier

调用流程

分析过程

下好2.1版本的fop，发现它这个组件连classpath都没弄好....同时也缺失了很多依赖，如果想要源码包的所有代码都能够跑起来的话，需要花费一些时间去将他们慢慢调好

组件里有用servlet生成PDF的例子，所以我们直接去看这一部分吧
路径：

直接看 doGet 函数

接受了三个参数的传入，参数名分别是：

renderXML 这个函数名这么明显，那么选择进入 xmlParam != null 的条件

跟入 renderXML

convertString2Source 是将字符串转换为 Source（也就是由文件名获取文件资源）
transformer 是根据 xsltSrc ，也就是指定的 xsl 文件资源生成的，然后 transformer 被带入了 render 函数里

我们先去看看 transformer 是啥类型的，跟进 newTransformer

发现是一个接口，并且我们目前没法确定 transFactory 是啥类型的....返回去看看

transFactory 在 servlet 的 init 函数中做了初始化

继续跟进

找到路径了，那么newTransfomer 函数生成的 transformer 也应该是 com.sun.org.apache.xalan.internal.xsltc.trax 这个路径

那就应该是 com.sun.org.apache.xalan.internal.xsltc.trax.TransformerImpl 这个类

uriResolver 也在 init 函数中初始化过

现在继续跟进 render 函数

因为 xml 文件是我们指定的，所以需要盯紧它，也就是在 render 中的 src 变量，如上图，传入了 transform 函数中，之前分析过 transformer
是啥类型的，跟过去

（截取部分代码）

```
@Override
public void transform(Source source, Result result)
   throws TransformerException
{
   if (!_isIdentity) {
       if (_translet == null) {
           ErrorMsg err = new ErrorMsg(ErrorMsg.JAXP_NO_TRANSLET_ERR);
           throw new TransformerException(err.toString());
       }
[.....]
   transform(source, toHandler, _encoding);
[.....]
```

继续跟着 source 走，跟进 transform

第一个 if 的地方，首先 source 是 StreamSource 类型的，但是它并不为空，所以不满足条件，直接跳过

第二个 if ，是通过动态调试得知 _isIdentity 是为 false 的（其实这里的影响不大，因为都最终会造成 xxe）

跟进 getDOM

跟进 getDTM

由于代码太多，只截取片段
两个布尔型变量分别表示 是否为 SAXSource ，是否为 StreamSource 类型，我们已知是 StreamSource 所以会进入下面的 if 判断中，并且获得了 XMLReader

如上图，在后续的流程中，并未采取一些防护措施，最终导致了 xxe

测试

首先让程序跑起来，有很多点。它自己有一个客户端，命令行形式的，然后我又找到一个用来展示其用法的实例

指定好路径就行

payload.xml 里是这样的

效果如下：

资料来源：
漏洞信息：https://www.securityfocus.com/bid/97947
FOP的简单使用：http://blog.csdn.net/youjianbo_han_87/article/details/2564642

点击收藏 | 0 关注 | 1
上一篇：AlphaJump - 如何用机器... 下一篇：Pwn with File结构体（四）
1. 0 条回复
   - 动动手指，沙发就是你的了！

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