CVE-2019-0227: Apache Axis RCE

Hulk / 2019-04-10 18:00:00 / 浏览数 13803 安全技术 漏洞分析 顶(0) 踩(0)

概述

Apache Axis™是一个简单对象访问协议（SOAP）引擎。在最近的一次红队行动中，我们发现目标装有老版本的Apache Axis（1.4）。现在较新的有Apache Axis2, Apache CXF,和Metro等。尽管Apache
Axis已经过时，但它仍然在许多情况下被使用，例如使用Axis构造的项目难以重写或者项目中含有使用SOAP编码的服务。

我们的目标仍在使用过时的版本，因此我们觉得值得深入挖掘，看看是否有可利用的漏洞。最后，我们找到了一个RCE漏洞，该漏洞是由于在默认的示例中使用了过期的硬编

Axis

如果你在服务器的Apache Axis或Axis2的找到服务端请求伪造（SSRF）漏洞，你也可能实现目标服务器的代码执行。在Ambionics Security的博客文章中有类似的介绍。因为涉及到产权保护，我不会介绍那篇文章的太多细节，总而言之：Axis以管理员权限处理localhost的请求，攻击者可以通过SSRF漏洞GET请求部分来伪装成localhost用户。

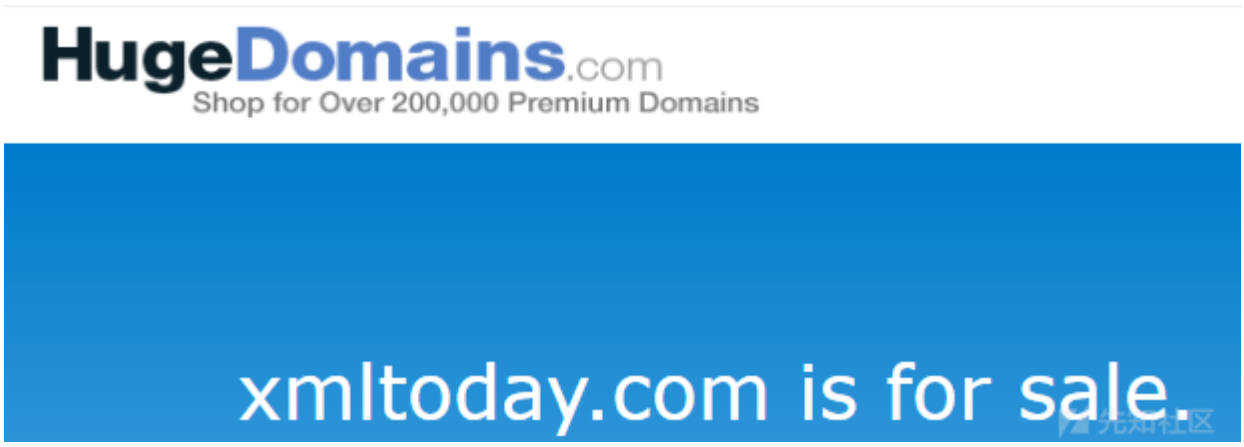
漏洞发现

根据前面我们的结论，我们应该在Axis默认或核心代码部分找出一个SSRF漏洞。在Axis默认安装程序中，会安装一个名为"StockQuoteService.jws"的默认示例web服务。这Web服务上做些什么。这里我们的示例web服务可以从外部网络的URL中获取股票价格。查看服务器中的代码，可以看到该服务发送一个HTTP请求至www.xmltoday.com来

```
Document doc = null ;

doc = XMLUtils.newDocument( "http://www.xmltoday.com/examples/" +
                            "stockquote/getxmlquote.vep?s="+symbol );
```


`XMLUtils.newDocument`用于从解析的目标域名中检索XML文档。由于用户可以控制发送给www.xmltoday.com的`symbol`字符，我的第一个想法是看看返回什么类型的数



www.xmltoday.com正在出售，所以这意味着我们可以购买它，然后将它设置重定向到某个精心构造的`localhost`URL。组合这点还有SSRF与RCE的一些小技巧，我们也许

```
HttpURLConnection uconn = (HttpURLConnection) connection;
String userinfo = wsdlurl.getUserInfo();
uconn.setRequestMethod("GET");
uconn.setAllowUserInteraction(false);
uconn.setDefaultUseCaches(false);
uconn.setDoInput(true);
uconn.setDoOutput(false);
uconn.setInstanceFollowRedirects(true);
uconn.setUseCaches(false);
```

查看Axis源码中的XMLutils部分，我们可以发现`setInstanceFollowRedirects`属性设置为`ture`。从而，我们确定了`XMLUtils.newDocument`函数将会遵循重定向流程

为了验证，我们购买了`www.xmltoday.com`域名，然后能够获取所有安装有Apache
Axis服务器的任意代码执行权限。同时，我们也防止了有人购买这个域名攻击其他网站。

其他攻击方法

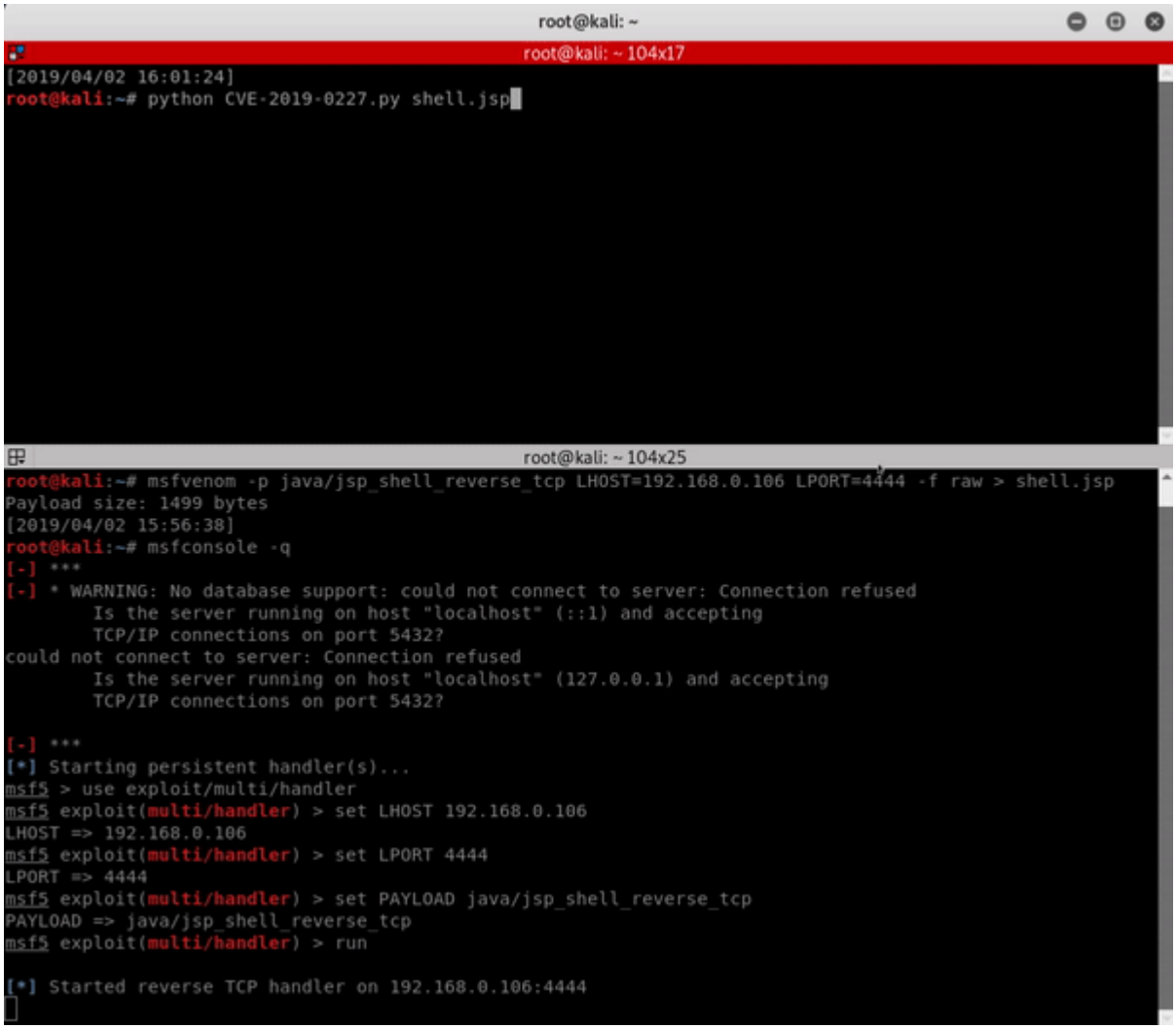
拥有这个域名的使用权其实并不是滥用`StockQuoteService.jws`和Axis服务器内部请求的唯一方法。由于请求通过HTTP实现，这意味攻击者（与Axis处于同一网段）能够

攻击步骤：

- ARP向目标Axis服务器投毒
- 拦截转发所有流量到你的web服务器
- 筛选，重定向到某个精心构造的`localhost`URL（属于Axis服务）
- 触发HTTP请求，然后重定向到`StockQuoteService.jws`（可控）

演示

在安装了Axis1.4的Apache Tomcat 8.5上，我们利用其默认自带的`StockQuoteService.jws`验证触发了该漏洞。如下gif所示：



Poc

MITM攻击的漏洞概念证明已放至Github

结论

值得注意的是，我们在Axis2上至今仍没有发现会发出HTTP请求的默认服务。如果你发现运行在Axis2服务器上的某个服务会发出HTTP请求，或许它也是可利用的。

如果你仍然在使用Axis服务，请删除Axis根目录的`StockQuoteService.jws`。同时，请确保你运行在Axis或Axis2上的任何服务或库不执行HTTP请求或者允许用户发出HT

时间表

01/15/2019 - 向Apache报告漏洞

01/27/2019 - Apache确认漏洞并接受报告

03/12/2019 - Apache推出了SSRF补丁

04/02/2019 - Apache签署CVE-2019-0227

文章来源：
https://rhinosecuritylabs.com/application-security/cve-2019-0227-expired-domain-rce-apache-axis/

上一篇：勒索攻击猖獗，在云上如何应对这位"... 下一篇：bypass open_based...
1. 0 条回复
   - 动动手指，沙发就是你的了！