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="Jc6/Jhsoft.Web.login" && body="CloseWindowNoAsk")|| header="Path=/je6"|| (body="JC6@和协同管理平台" && body="src=\"jc6/platform")|| body="window.location = \"JHSoft.MobileApp/Default.htm\";"|| banner="Path=/je6"|

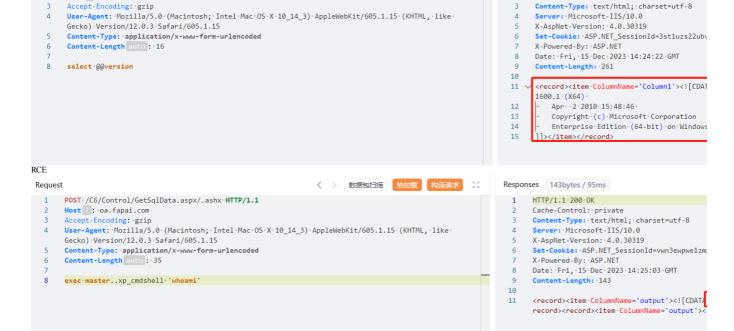
漏洞复现:

```
payload:
```

Request

POST /C6/Control/GetSqlData.aspx/.ashx HTTP/1.1

Host ?: oa.fapai.com



〈 〉 数据包扫描 热加载 构造请求 💥

Responses 261bytes / 67ms

HTTP/1.1.200.0K

Cache-Control: private

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。