

# Unauthorized access vulnerability in Ruijie RG-NBS2009G-P switch

## 1. Impact of vulnerabilities

RG-NBS2009G-P

## 2. Vulnerability location

/system/passwdManage.htm

## 3. Vulnerability recurrence

### Case 1

**Vulnerability Address:** <http://119.123.222.209:8888/>

#### Vulnerability details:

Without logging in, accessing the /system/passwdManage.htm page will cause unauthorized operation of the page, and then directly modify the Web and Telnet password of the switch.

← → ↻ 🔍 ⚙️ ⚠️ 不安全 119.123.222.209:8888/system/passwdManage.htm ☆

修改超级用户密码

提示: 如果您设置了新的Web登录密码, 则在设置之后使用新密码重新登录。 密码只能由字母、数字和下划线组成

旧密码:

新密码:

确认新密码:

确定修改 清空

telnet登录密码

新密码:

确认新密码:

确定修改 清空



## Case 2

**Vulnerability Address:** <http://119.123.222.65:8888/>

### Vulnerability details:

Without logging in, accessing the `/system/passwdManage.htm` page will cause unauthorized operation of the page, and then directly modify the Web and Telnet password of the switch.



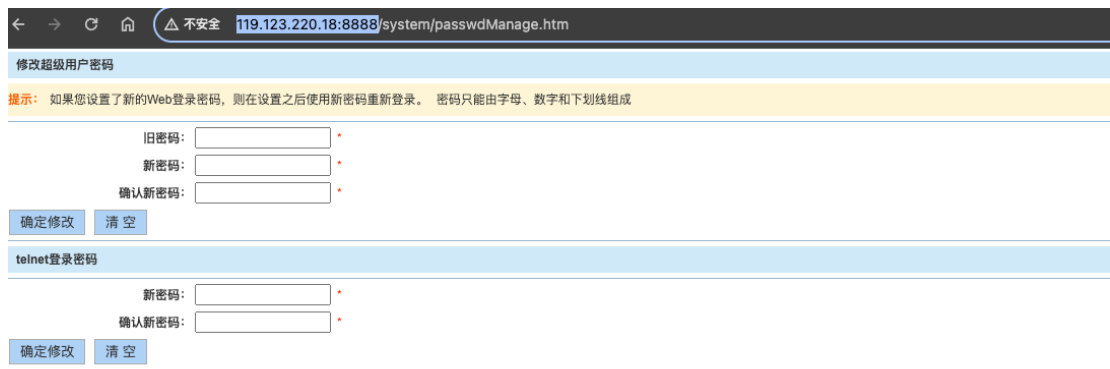


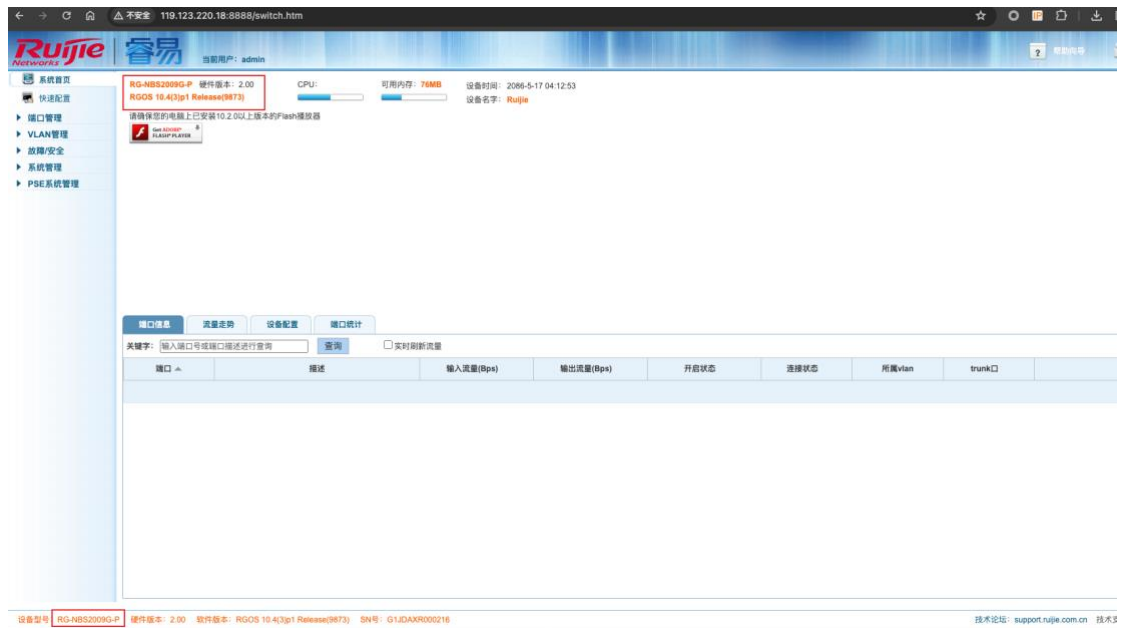
### Case 3

**Vulnerability Address:** <http://119.123.220.18:8888/>

#### Vulnerability details:

Without logging in, accessing the /system/passwdManage.htm page will cause unauthorized operation of the page, and then directly modify the Web and Telnet password of the switch.





## Other vulnerable urls

<http://119.123.223.194:8888/>



<http://119.123.220.18:8886>

锐捷网络 Ruijie Networks 睿易 当前用户: admin

系统首页 快速配置 端口管理 VLAN管理 故障/安全 系统管理 PSE系统管理

RG-NBS2009G-P 硬件版本: 2.00 CPU: 80% 可用内存: 76MB 设备时间: 1970-1-1 07:05:28  
RGOS 10.4(3)p1 Release(9873) 设备名字: Ruijie

请确保您的电脑上已安装10.2.0以上版本的Flash播放器

Get Adobe Flash Player

端口信息 流量走势 设备配置 端口统计

关键字: 输入端口号或端口描述进行查询 查询 ☐ 实时刷新流量

端口	描述	输入流量(Bps)	输出流量(Bps)	开启状态
----	----	-----------	-----------	------

<http://119.123.223.195:9000/>

锐捷交换机 锐捷网络 Ruijie Networks 睿易 当前用户: admin

系统首页 快速配置 端口管理 VLAN管理 故障/安全 系统管理 PSE系统管理

RG-NBS2009G-P 硬件版本: 2.00 CPU: 79% 可用内存: 76MB 设备时间: 1970-1-1 01:01:22  
RGOS 10.4(3)p1 Release(9873) 设备名字: Ruijie

请确保您的电脑上已安装10.2.0以上版本的Flash播放器

Get Adobe Flash Player

<http://119.123.223.195:8888/index.htm>



<http://qddeagry.v3n.pkoplink.com:8886>



<http://dqdeagps.v3n.pkoplink.com:8886/>

