网络安全预警通报

2023 年第 3 期 （总第 40 期）

西安交通大学网络信息中心 2023 年 7 月 25 日

【预警类型】 **高危预警**

【预警内容】

关于锐捷 EG/NBR 部分型号历史漏洞的说明

一、漏洞概述

近期，锐捷公司收到反馈个别用户因 EG/NBR 产品历史漏洞遭到攻击。经排查，此安全漏洞存在于 EG/NBR 部分产品的特定历史版本（即 11.x 版本存在远程代码执行漏洞）。已于 2020 年 5 月发现并第一时间发布了漏洞规避方案与修复版本，并通过产品云端、锐捷官网及国家公开平台（CNVD）发布了漏洞通告，为客户提供版本升级等技术支持，协助用户开展漏洞修复工作。

（详见：https://www.ruijie.com.cn/gy/xw-aqtg-zw/85638/）

为了保护各单位设备的安全运行，建议您根据使用的产品型号，下载对应版本进行升级，升级后即可避免受到漏洞影响。

二、 漏洞详情

在设备 Web 管理权限未进行访问限制时才会受此漏洞影响（尤其设备 Web 管理权限开放到互联网情形下风险更高），在此特定场景下攻击者可利用漏洞对 EG/NBR 设备进行高危操作。

漏洞影响范围：

系列	型号
RG-NBR 系列	RG-NBR108G-P、RG-NBR1000G-E、RG-NBR1300G-E、RG-NBR1700G-E、RG-NBR2100G-E、RG-NBR2500D-E、RG-NBR3000D-E、RG-NBR6120-E、RG-NBR6135-E、RG-NBR6205-E、RG-NBR6210-E、RG-NBR6215-E、RG-NBR800G、RG-NBR950G、RG-NBR1000G-C/ RG-NBR2000G-C/ RG-NBR3000G-S
RG-EG 系列	RG-EG1000C、RG-EG2000F、RG-EG2000K、RG-EG2000L、RG-EG2000CE、 RG-EG2000SE、RG-EG2000GE、RG-EG2000XE、RG-EG2000UE、RG-EG3000CE、RG-EG3000SE、RG-EG3000GE、RG-EG3000ME、RG-EG3000UE、RG-EG3000XE、RG-EG2100-P、RG-EG3210、RG-EG3220、RG-EG3230、RG-EG3250

涉及软件版本

11.9(4)B12P1（含）之前版本，2020 年 5 月之后正式发布的版本均不受影响。

三、 处置建议

1.建议使用 RGOS 11.9(6)B13P1 及之后正式版行系统升级，版本获取链接：https://www.ruijie.com.cn/fw/rj/90787/

2.关闭 Web 访问权限或设置 Web 访问白名单。

3.升级后修改设备 Web 管理密码、SSH 密码、TELNET 密码、VPN 密码（包括 VPN 用户的密码）。密码强度要求至少 8 位、由大小写字母、数字、特殊符号组成。

参考链接：

https://www.ruijie.com.cn/gy/xw-aqtg-gw/91876/