

知 关于ERG1_ERG2系列路由器存在未授权访问漏洞的技术公告

软件相关 马文斌 2022-06-09 发表

公告级别

客户级别

公告类别

预警

操作要求

软件升级

产品型号

ERG1系列路由

器: ER2100、ER2100n、ER2100v2、ER2210C、ER3100、ER3108G、ER3108GW、ER3200、ER3260、ER3280G、ER5100、ER5200、ER6300、ER8300系列

ERG2系列路由器: ER2200G2、ER3100G2、ER3200G2、ER3260G2、ER5100G2、ER5200G2、ER6300G2、ER8300G2、ER8300G2-X、ERG2-450W、ERG2-1200W、ERG2-1350W、NR-1200W系列

涉及版本

ERG1系列路由器：所有版本均涉及

ER2200G2、ERG2-450W、ERG2-1200W、ERG2-1350W、NR1200W系列路由器：R1113（不含）之前版本

ER3100G2、ER3200G2、ER3260G2、ER5100G2、ER5200G2、ER6300G2、ER8300G2、ER8300G2-X系列路由器：R1122（不含）之前版本

问题描述

设备开启远程管理情况下，攻击者可使用特殊的post请求对设备发起攻击，绕过设备安全认证流程，获取设备敏感信息

原因分析

ERG1和ERG2设备涉及前台未授权访问的漏洞问题，攻击者可利用这个漏洞，使用特殊post请求对设备发起攻击，绕过设备安全认证流程，获取设备配置以及密码等敏感信息

规避措施/解决方案

规避措施:

关闭设备远程Web管理和Telnet管理功能

解决方案:

ER2200G2、ERG2-450W、ERG2-1200W、ERG2-1350W、NR1200W可升级至R1113版本解决

ER3100G2、ER3200G2、ER3260G2、ER5100G2、ER5200G2、ER6300G2、ER8300G2、ER8300G2-X可升级至R1122版本解决

ERG1系列路由器不再发布新版本，可采用上述规避方法

