

关于中低端路由器ERG1/ERG2设备存在命令行注入及敏感信息泄露漏洞问题的技术公告

Telnet 朱玉广 2021-09-23 发表

问题描述

公告类别	预警
操作要求	学习预防、版本升级

【产品型号】

中低端路由器	系列
ERG1	ER3100、ER3200、ER3260、ER5100、ER5200、ER8300等系列
ERG2	ER2200G2、ER3100G2、ER3200G2、ER3260G2、ER5100G2、ER5200G2、ER6300G2、ER8300G2、ER8300G2-X、ERG2-450W、ERG2-1200W、ERG2-1350W等系列

【涉及版本】

R1120 (不含) 之前版本

【漏洞问题描述】

上述设备运行R1120之前版本，存在命令行注入安全漏洞和敏感信息泄露安全漏洞问题。具体如下：

命令行注入安全漏洞，攻击者可以通过该途径打开设备telnet,也可将普通web用户提权到root用户。

敏感信息泄露安全漏洞，攻击者可以通过该途径绕过安全认证获取设备的敏感信息，比如配置信息以及密码信息。

原因分析

不涉及

规避措施/解决方案

规避方案：关闭设备远程TELNET和HTTP管理功能。

解决方案：ERG2可升级至R1120及之后版本解决，ERG1暂无新版本解决。

