RPC3111产品中信息篡改漏洞

发布日期：2022年3月9日
最后更新日期：2026年1月6日
北京蓝普锋科技有限公司

■概述

目前网络安全产品RPC3000系列PLC已知存在漏洞有以下两处，MODBUS TCP访问漏洞和OPENSSH版本漏洞，导致产品中的信息被泄露或篡改 。

■受影响的产品

以下产品受到影响：

CPU模块	产品名称	版本
RPC3000系列	RPC3111	所有版本

■描述

①MODBUS TCP访问漏洞

由于采用标准协议Modbus Tcp，其默认端口为502，攻击者利用现有协议和端口读取或篡改设备参数，运行状态信息。

②OPENSSH版本漏洞

目前设备使用Openssh 10.0版本，低于10.1版本可能提示安全缺陷（Multiple Vulnerabilities），此缺陷主要是当用户在openssh中配置ProxyCommand才会引入此安全风险，本设备没有配置ProxyCommand，因此无需担心。

■影响

如果恶意攻击者利用这些漏洞，未经过身份验证的攻击者可能能够登录相关产品，或导致产品中的信息被泄露或篡改。

■对策

①MODBUS TCP访问漏洞：用户可以使用本设备iptables防火墙和白名单名单机制规避此风险，具体参考手册。

②OPENSSH版本漏洞：禁止用户配置ProxyCommand。

■联系方式

请联系本公司的销售人员。
北京蓝普锋科技有限公司
http://www.runpower.cn/jswd.php

■更新历史记录

2026年1月5日

将OPENSSH版本漏洞增至漏洞警告。