**国家信息安全漏洞共享平台(CNVD)漏洞通报**

**关于锐易网关存在弱口令漏洞的情况通报**

国家互联网应急中心（CNCERT） 2023年1月13日

## 漏洞描述

设备:锐捷网络锐易网关

弱口令为:admin:admin

影响版本包括:

BCOS V2.5.8

BCOS V2.5.10

BCOS V2.5.10p3

BCOS V2.5.10p2

BCOS V2.5T2

漏洞验证

183.189.193.96:6060



123.52.12.134:6060



<http://60.189.175.198:6060/>



<http://36.24.83.54:8000/>



<http://61.190.101.24:9001/>

<http://123.234.194.236:6060/>

<http://123.113.145.247:6060/>

<http://125.32.246.225:6060/>

<http://113.237.28.114:8000/>

<http://221.8.152.218:6060/>

<http://111.3.154.69:6060/>

**关于CNVD**

国家信息安全漏洞共享平台（China National Vulnerability Database，简称CNVD）是由CNCERT联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的国家网络安全漏洞库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

**关于CNCERT**

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是CNCERT或CNCERT/CC），成立于2002年9月，为非政府非盈利的网络安全技术中心，是我国计算机网络应急处理体系中的牵头单位。

作为国家级应急中心，CNCERT的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537