Digital India Power To Empower

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Full Member
Operational Member
Accredited Member
Global Research Partner
Associate Partner
CVE Numbering Authority (CNA)

Directions by CERT-In under Section 70B, Information Technology Act 2000

Guidelines on Information Security Practices for Government Entities

15 Elemental Cyber Defense Controls for Micro, Small, and Medium Enterprises (MSMEs) NEW

Technical Guidelines on SBOM, QBOM & CBOM, AIBOM and HBOM Version 2.0 NEW

Cyber Security Guidelines for Smart City Infrastructure NEW

Cyber Security Framework and Guidelines for Space including Satellite Communication NEW

ABOUT CERT-In
- Client's /Citizen's Charter
- Roles & Functions
- Advisory Committee
- Act/Rules/Regulations
- Internal Complaint Committee (ICC)
- RFC2350
- Press
- Tender
- Subscribe Mailing List
- Contact Us

REPORTING
- Incident Reporting
- Vulnerability Reporting
- Feedback

KNOWLEDGEBASE
- Guidelines
- Presentations
- White Papers
- Annual Report

Home - Vulnerability Notes

CERT-In Vulnerability Note CIVN-2026-0200
Multiple Vulnerabilities in Quantum Networks Router

Original Issue Date:April 21, 2026

Severity Rating: HIGH

Systems Affected

- Quantum Networks Router QN-I-470 - Firmware version 6.1.1.B1

Overview

Multiple vulnerabilities have been reported in the Quantum Networks router, which could allow an attacker to execute arbitrary code, perform brute-force attacks, gain unauthorized administrative access or access sensitive information on the targeted device.

Target Audience:
End-users/ Administrators of Quantum Networks router

Risk Assessment:
Risk of remote code execution, brute-force attack, unauthorized administrative access and potential sensitive information.

Impact Assessment:
Potential for remote code execution, information disclosure and device compromise.

Description

The Quantum Networks Router QN-I-470 is a dual-band Wi-Fi 6 (802.11ax) indoor access point designed to provide wireless network connectivity.

1. Command Injection Vulnerability (CVE-2026-41036)

This vulnerability exists in Quantum Networks router due to inadequate sanitization of user-supplied input in the management CLI interface. An authenticated remote attacker could exploit this vulnerability by injecting arbitrary OS commands on the targeted device.
Successful exploitation of this vulnerability could allow the attacker to perform remote code execution with root privileges on the targeted device.

2. Missing Rate Limiting Vulnerability (CVE-2026-41037)

This vulnerability exists in Quantum Networks router due missing rate limiting and captcha protection for failed login attempts in the web management interface. An attacker on the same network could exploit this vulnerability by performing brute force attacks against the administrative account on the targeted device to gain unauthorized access with root privileges.

3. Weak Password Policy Vulnerability (CVE-2026-41038)

This vulnerability exists in Quantum Networks router due to lack of enforcement of strong password policies in the web management interface. An attacker on the same network could exploit this vulnerability by performing password guessing or brute-force attacks against user accounts on the targeted device.
Successful exploitation of this vulnerability could allow the attacker to gain unauthorized access to the targeted device.

4. Information Disclosure Vulnerability (CVE-2026-41039)

This vulnerability exists in Quantum Networks router due to improper access control and insecure default configuration in the web management interface. An unauthenticated attacker could exploit this vulnerability by accessing exposed API endpoints on the targeted device.
Successful exploitation of this vulnerability could allow the attacker to access sensitive information, including internal endpoints, scripts and directories on the targeted device.

Credits

These vulnerabilities are reported by the following team of security researchers:

1. Rakesh Elamaran, Karthik D, Mir Mohammed Kaif, Joel William, Bajino Viju and Kalpana B N (CVE-2026-41036)
2. Rakesh Elamaran, Stalin S, Janish Andrin J, Kali Vignesh SM, Arkino Robilin R and Kalpana B N (CVE-2026-41037)
3. Rakesh Elamaran, Praveen S, Vignesh T, Shervin Bruce, Infant Raj R and Kalpana B N (CVE-2026-41038)
4. Rakesh Elamaran, Joel William A, Bajino Viju, Stalin S, Janish Andrin J and Kalpana B N (CVE-2026-41039)

Solution

Upgrade Quantum Networks Router QN-I-470 to latest firmware version 7.5.4.B9:
https://www.qntmnet.com/wp-content/uploads/2026/04/QN-I-470-7.5.4.B9.qntm?ver=1775552129

Vendor Information

Quantum Networks
https://www.qntmnet.com/wp-content/uploads/2026/04/QN-I-470-7.5.4.B9.qntm?ver=1775552129

References

Quantum Networks
https://www.qntmnet.com/wp-content/uploads/2026/04/QN-I-470-7.5.4.B9.qntm?ver=1775552129

CVE Name

CVE-2026-41036
CVE-2026-41037

RECRUITMENTS NEW
Security Tips for Common Users NEW
ADVISORIES
VULNERABILITY NOTES
RELATED LINKS
- World CERTs
- Antivirus Resources
- FAQ

Performance Management
india.gov.in
Public Grievances (DAR&PG)
mygov मेरी सरकार
data.gov.in Open Government Data (OGD) Platform India
ISAC Power NEW
राष्ट्रीय मतदाता सेवा पोर्टल NATIONAL VOTERS' SERVICES PORTAL www.eci.nic.in | www.nvsp.in
Modes of Digital Payments
DIGITAL PAYMENT suraksha
RTI
Collaboration and Engaging with CERT-In
State/Sectoral CSIRT NEW

CVE-2026-41038
CVE-2026-41039

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-22902657

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India