مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

# Critical Vulnerability in QNAP QVR Pro

Tracking #:432318637

Date:22-03-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

**TLP: WHITE**

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in QNAP QVR Pro that could allow unauthorized remote access to affected systems.

## TECHNICAL DETAILS:

A critical security vulnerability has been identified in QVR Pro. The flaw could allow remote attackers to gain unauthorized access to affected systems due to missing authentication controls on critical functions.

**Vulnerability Details**

- **CVE ID:** CVE-2026-22898
- **Severity:** Critical
- The vulnerability is caused by missing authentication for a critical function in QVR Pro. An unauthenticated remote attacker can exploit this flaw to gain unauthorized access to the system, potentially leading to compromise of surveillance data and system control.

**Affected Product**

- QVR Pro 2.7.x

**Fixed Versions**

- QVR Pro 2.7.4.1485 and later

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by QNAP.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://www.qnap.com/en/security-advisory/qsa-26-07