مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in ARC Solo Broadcasting Devices

Tracking #:432317585

Date:11-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical authentication bypass vulnerability in ARC Solo monitoring and control units, widely used in broadcasting operations. This flaw allows remote attackers to change device passwords without valid credentials, potentially leading to full device takeover.

TECHNICAL DETAILS:

A critical authentication bypass vulnerability (CVE-2025-5095) has been identified in Burk Technology's ARC Solo broadcast control devices. This vulnerability allows remote attackers to change device passwords without authentication, leading to potential unauthorized device takeover, operator lockout, and operational disruption.

Vulnerability Details:

- **CVE-2025-5095**
- **CVSS Base Score**: 9.8 Critical
- The ARC Solo's password change mechanism can be accessed without proper authentication or session validation. An attacker can send a crafted HTTP request directly to the password change endpoint, bypassing login requirements.
- Exploitation of this vulnerability can lead to:
  - Unauthorized device access
  - Lockout of legitimate administrators
  - Operational disruption in broadcasting networks

Affected Versions:

- ARC Solo prior to v1.0.62

Fixed Versions:

- ARC Solo v1.0.62 and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the fixed updates at the earliest.

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.cisa.gov/news-events/ics-advisories/icsa-25-219-03