مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerabilities in D-Link IP Cameras

Tracking #:432317579
Date:08-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed an active exploitation campaign targeting legacy D-Link IP cameras and NVRs, posing a significant threat to organizational network integrity. These vulnerabilities could enable unauthorized access, remote code execution, and persistent device compromise.

TECHNICAL DETAILS:

Vulnerability Details:

1. **CVE-2020-25078 – Admin Credential Disclosure**
   - **Affected Devices**: D-Link DCS-2530L, DCS-2670L
   - **Description**: An unauthenticated endpoint (/config/getuser) allows remote attackers to retrieve administrator passwords.
   - **Fixed Versions**:
     - DCS-2530L: Firmware v1.07.00
     - DCS-2670L: Firmware v2.03.00
   - **Severity**: High
   - **Impact**: Enables attackers to gain admin access without authentication, potentially leading to full device compromise.

2. **CVE-2020-25079 – Authenticated Command Injection**
   - **Affected Devices**: D-Link DCS-2530L, DCS-2670L
   - **Description**: Authenticated users can exploit a command injection vulnerability via the cgi-bin/ddns_enc.cgi endpoint.
   - **Fixed Versions**:
     - DCS-2530L: Firmware v1.07.00
     - DCS-2670L: Firmware v2.03.00
   - **Severity**: High
   - **Impact**: Can be used as a second-stage exploit after CVE-2020-25078 to execute arbitrary commands remotely.

3. **CVE-2022-40799 – Persistent Backdoor via Startup Script**
   - **Affected Device**: D-Link DNR-322L
   - **Description**: Exploits the backup/restore feature to modify the rc.init.sh startup script, allowing persistent code execution on boot.
   - **Fixed Version**: None (Device is End-of-Life)
   - **Severity**: Critical
   - **Impact**: Allows attackers to maintain persistent access and control over the device. A **publicly available proof-of-concept** increases the risk of exploitation.

RECOMMENDATIONS:

The UAE Cyber Security Councils recommends replacing the affected models with supported alternatives, and applying the fixed updates, where applicable.

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/alerts/2025/08/05/cisa-adds-three-known-exploited-vulnerabilities-catalog