مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Path Traversal Vulnerability in D-Link Routers
Tracking #:432317428
Date:30-06-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in D-Link DIR-859 Wi-Fi routers which has been actively exploited in the wild. The vulnerability allowed attackers to gain unauthorized access and potentially full control over affected devices.

TECHNICAL DETAILS:

A critical unauthenticated path traversal vulnerability (**CVE-2024-0769**) affects all hardware and firmware versions of the D-Link DIR-859 router. Exploitable via the /hedwig.cgi HTTP POST handler, this flaw allows remote attackers to access sensitive configuration files, potentially exposing account credentials and enabling full device takeover. As the DIR-859 reached end-of-life in December 2020, D-Link will not issue a fix. Users are strongly advised to retire and replace the device immediately to avoid permanent security risks.

Vulnerability Details:

- **CVE-2024-0769**
  - **Severity:** Critical
  - **CVSS v4.0 Base Score:** 9.8
  - **Impact:** This allows them to leak session data, retrieve account names and passwords, and potentially escalate privileges to take full control of the device.
  - **Exploitation Status:** Actively exploited.

Affected Versions:
- All versions of D-Link DIR-859 router.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends immediate retirement and replacement of all D-Link DIR-859 routers to mitigate the critical security risks posed by the vulnerability.

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://nvd.nist.gov/vuln/detail/cve-2024-0769