مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in D-Link Routers

Tracking #:432318841

Date:25-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical command injection vulnerability, CVE-2025-29635, is being actively exploited in the wild to compromise end-of-life D-Link DIR-823X routers.

TECHNICAL DETAILS:

A critical command injection vulnerability, CVE-2025-29635, is being actively exploited in the wild to compromise end-of-life D-Link DIR-823X routers. Threat actors are leveraging this flaw to deploy variants of the Mirai botnet, enabling large-scale distributed denial-of-service (DDoS) attacks and persistent device compromise.

Vulnerability Details

- CVE ID: CVE-2025-29635
- Vulnerability Type: Command Injection
- Affected Devices: D-Link DIR-823X series routers
- Affected Firmware Versions: 240126, 24082
- Status: Devices officially End-of-Life (EOL) as of September 2025
- Attack Vector: Remote (HTTP POST request)
- Authentication Required: Not effectively enforced

Indicators of Compromise (IOCs)

Malicious IPs

- 88.214.20.14
- 64.89.161.130

File Hashes (SHA256)

- 2ca4b70e84787144574bfdb85a0092f3ebf524bb78febdd28d4c832b53fe100
- be902e86ec68515e23a3387a21e80d098d258223ce562598c27ee6d89b83ff2b
- d232c0960f24ba4bb369821b1bf2836d9e576a34fa3ddca2618c80b2f54277f7
- 7792f5c1d5c6c6415732ba0f63328549e19cc9c182c258c17b97b77fdb5541b8
- 72eff03b8573329818b38185074aa763e99d15f5709fecc44f9afece21dc06d8

RECOMMENDATIONS:

Decommission affected devices

- Replace all D-Link DIR-823X routers (no patches available due to EOL status).

Block known malicious IPs

- Enforce network-level blocking for identified IOC addresses.

Monitor outbound traffic

- Detect unusual connections to unknown external hosts or high ports.

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.akamai.com/blog/security-research/cve-2025-29635-mirai-campaign-targets-d-link-devices#iocs