مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

D-Link End-of-Life Routers Vulnerable to Botnet Exploits

Tracking #:432316695
Date:02-01-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that D-Link has issued a critical advisory, urging users to promptly retire and replace several legacy router models due to their vulnerability to botnet exploits.

TECHNICAL DETAILS:

D-Link has issued a critical advisory regarding several of its legacy router models that have reached End-of-Life (EOL) and End-of-Support (EOS) status. The company is strongly urging users to retire and replace these vulnerable devices due to the increasing threat of botnet attacks.

Affected Models and EOL Dates:

- **DIR-645**: All hardware revisions, EOL as of December 31, 2018.
- **DIR-806**: All hardware revisions, EOL as of February 1, 2016.
- **GO-RT-AC750**: All hardware revisions, EOL as of February 29, 2016.
- **DIR-845L**: All hardware revisions, EOL as of March 1, 2016.

Vulnerabilities and Exploits:

These routers are being targeted by two botnets known as "Ficora" and "Capsaicin". The botnets exploit multiple known vulnerabilities, including CVE-2015-2051, CVE-2019-10891, CVE-2022-37056, and CVE-2024-33112.

Once compromised, attackers leverage weaknesses in the D-Link Management Interface (HNAP) to execute malicious commands via the "GetDeviceSettings" action. These attacks can lead to:

- Theft of sensitive data.
- Execution of unauthorized shell scripts.
- Deployment of large-scale Distributed Denial-of-Service (DDoS) operations.

RECOMMENDATIONS:

- **Retire and replace** affected router models immediately
- Ensure devices have the latest available firmware
- Use unique and regularly updated passwords
- Enable robust Wi-Fi encryption

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://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10417