مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in D-Link routers

Tracking #:432318223

Date:09-01-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical flaw in legacy D-Link routers is being actively exploited, enabling attackers to control router settings and potentially compromise connected devices.

TECHNICAL DETAILS:

A critical security flaw affecting legacy D-Link DSL gateway routers has been actively exploited in the wild. The vulnerability allows unauthenticated remote attackers to execute arbitrary commands via the dnscfg.cgi endpoint, enabling full control over DNS settings and persistent compromise of downstream devices. Many impacted devices are end-of-life (EoL) and cannot be patched.

Vulnerability Details:

- **CVE-2026-0625**
- **CVSS v3.1 Score:** 9.3 (Critical)
- **Type:** Command Injection / Remote Code Execution
- Improper input validation in the dnscfg.cgi endpoint allows unauthenticated attackers to execute arbitrary commands and modify DNS settings, leading to full remote control of the router.

Impact:

- Unauthenticated remote code execution on vulnerable routers
- Unauthorized modification of DNS settings ("DNSChanger")
- Potential redirection, interception, or blocking of all network traffic downstream
- Persistent compromise for all connected devices

Affected Products (Legacy DSL Gateway Models):

- DSL-2640B – firmware <= 1.07
- DSL-2740R – firmware < 1.17
- DSL-2780B – firmware <= 1.01.14
- DSL-526B – firmware <= 2.01

Exploitation:

Active exploitation of this vulnerability has been observed targeting legacy firmware versions. Attackers can exploit the flaw without authentication or user interaction, allowing them to control DNS settings and potentially redirect all network traffic.

RECOMMENDATIONS:

- Replace legacy DSL gateways with supported devices.
- Monitor DNS settings for unauthorized changes.
- Keep firmware updated on supported devices.
- Audit connected devices for suspicious activity.
- Follow official D-Link updates for affected models and guidance.

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-2026-0625