Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-0625: A Decade-Long Risk in D-Link DSL Routers Enabling Full System Compromise

Date of Publication	Admiralty Code	TA Number
January 07, 2026	A1	TA2026005

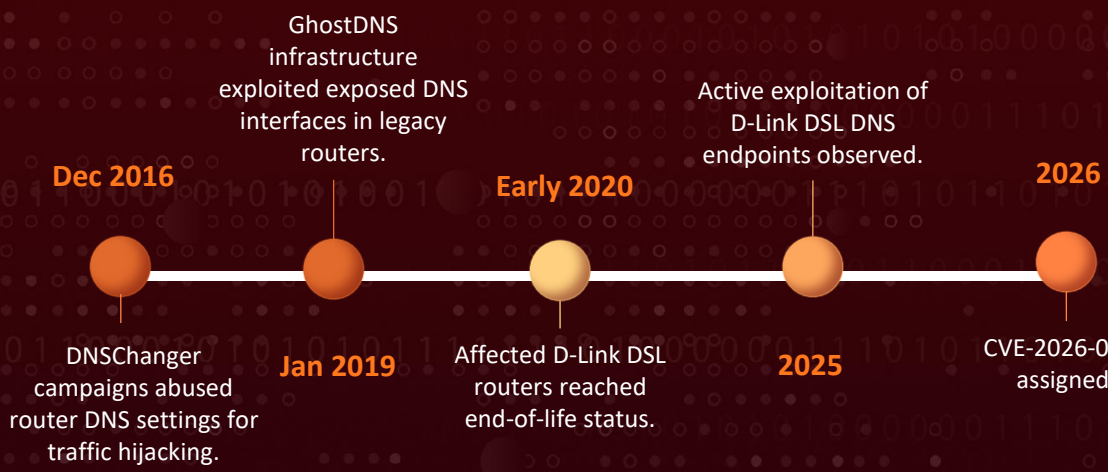
Summary

Attack Commenced: December 2016
Affected Products: D-Link DSL-2740R, D-Link DSL-2640B, D-Link DSL-2780B, D-Link DSL-526B
Malware: DNSChanger, GhostDNS
Impact: CVE-2026-0625 is a critical security flaw affecting several legacy D-Link DSL routers, where a weakness in the DNS configuration endpoint allows attackers to take full control of the device. By abusing poorly validated DNS inputs, remote threat actors can inject and execute system-level commands, effectively gaining complete access to the router. What makes this issue especially alarming is that it is actively being exploited, with confirmed activity observed in late 2025 and strong similarities to past DNSChanger attacks. Since the affected models reached end-of-life 6 years ago and will not receive patches, any organizations or individuals still using these devices remain highly exposed, making immediate device replacement the only safe course of action.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-0625	D-Link DSL Gateway Command Injection via DNS Configuration Endpoint Vulnerability	D-Link DSL Gateway Routers	✓	✗	EOL

Exploitation Timeline



Vulnerability Details

#1

CVE-2026-0625 a critical command injection flaw in the dnscfg.cgi endpoint found across multiple legacy D-Link DSL gateway devices. This endpoint handles DNS configuration requests submitted through the router's web-based management interface. The vulnerability originates from weak input validation, where user-supplied DNS parameters are not properly sanitized before being processed by the underlying system.

#2

As a result, specially crafted requests can embed malicious command sequences within DNS configuration fields. These commands are passed directly to the device's shell and executed with the same privileges as the web service, which on embedded Linux-based router firmware often equates to root-level access. This transforms what should be a simple configuration feature into a direct gateway for full system compromise.

#3

The risk is significantly amplified by the fact that the vulnerable endpoint is exposed without any authentication. Attackers do not need valid credentials or user interaction to exploit the flaw; a remote HTTP request is sufficient. This makes large-scale, automated exploitation highly feasible, particularly against internet-facing devices that remain widely deployed despite being end-of-life.

#4

This vulnerability also echoes past DNSChanger and GhostDNS campaigns were observed between December 2016 and January 2019, where attackers abused DNS settings to redirect traffic for phishing, ad fraud, and credential theft. However, CVE-2026-0625 goes far beyond DNS manipulation, enabling full command execution and long-term device takeover. Active exploitation has already been observed in the wild, confirming activity in late 2025. Given the ability to intercept all downstream traffic, deploy malware, and pivot deeper into connected networks, this issue is rated critical. D-Link strongly advises immediate retirement and replacement of affected devices, as continued operation poses a severe and ongoing security risk to both organizations and individual users.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-0625	D-Link DSL-526B (versions <= 2.01), D-Link DSL-2640B (versions <= 1.07), D-Link DSL-2740R (versions < 1.17), D-Link DSL-2780B (versions <= 1.01.14)	cpe:2.3:h:dlink:dsl:*:*:*:*:*:*:*	CWE-78

Recommendations

Asset Inventory and Identification: Conduct an immediate audit to identify all D-Link DSL-526B, DSL-2640B, DSL-2740R, and DSL-2780B devices within your environment. Document their network locations, configurations, and connectivity to critical systems.

Network Isolation: Immediately segment affected devices from critical network assets. Place vulnerable routers behind additional firewall controls or in isolated network zones to limit potential lateral movement in the event of a compromise.

Review DNS Settings: Verify current DNS server configurations on affected devices. Check for unauthorized DNS servers that may indicate prior compromise. Legitimate DNS servers include trusted providers like Google (8.8.8.8, 8.8.4.4) or Cloudflare (1.1.1.1).

Device Replacement Planning: Develop a prioritized replacement schedule for all affected end-of-life D-Link DSL gateways. Procure routers that actively support models that receive regular firmware and security updates.

Factory Reset with Verification: Perform factory resets on affected devices and reconfigure with strong, unique administrative passwords. Note that this does not eliminate the underlying vulnerability but may remove existing compromises.

Establish End-of-Life Policies: Implement organizational policies requiring retirement of network devices upon reaching end-of-life status. Track vendor support timelines proactively.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
	T1584: Compromise Infrastructure	T1584.002: DNS Server

Patch Details

No patches are available. The affected devices have reached end-of-life/end-of-service status as of early 2020 and will not receive security updates from D-Link.

Links:
https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10488

https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10068

References

https://www.vulncheck.com/advisories/dlink-dsl-command-injection-via-dns-configuration-endpoint

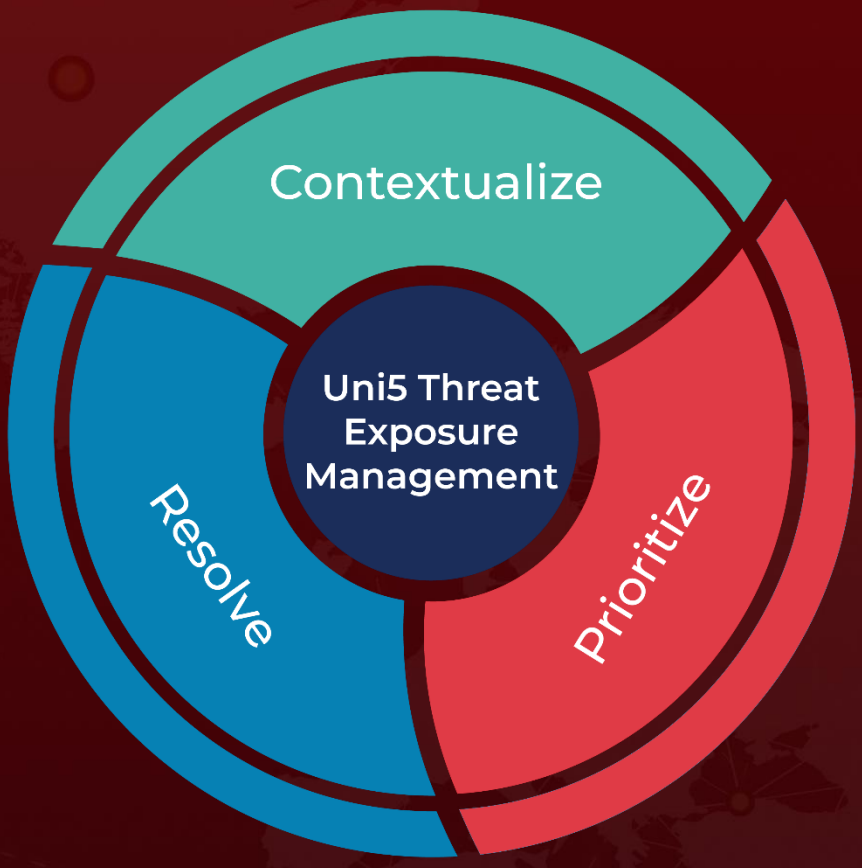
https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10488

https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10068

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 07, 2026 • 7:00 AM

More at www.hivepro.com