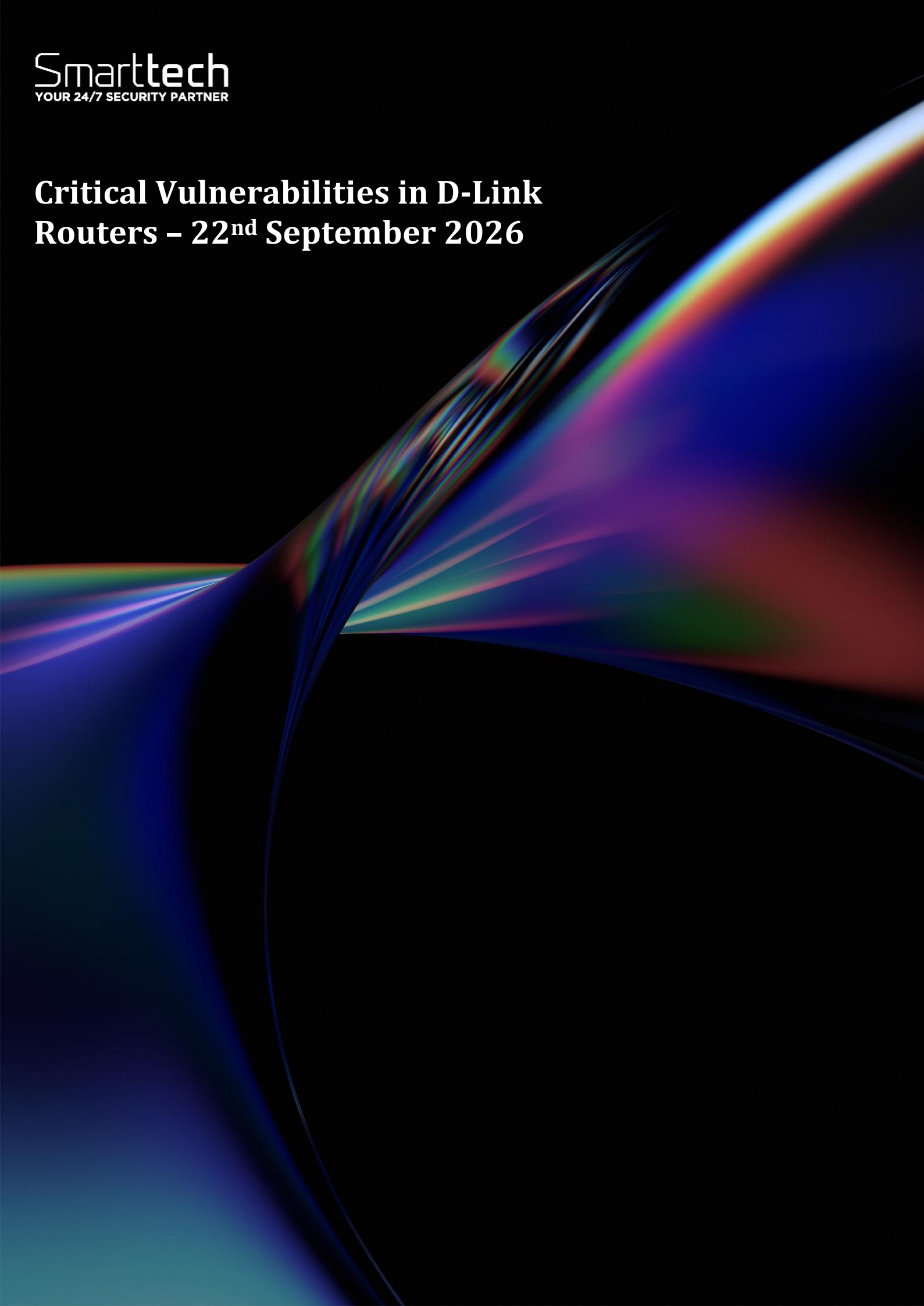
Smarttech
YOUR 24/7 SECURITY PARTNER

Critical Vulnerabilities in D-Link Routers – 22nd September 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	168
Authors	Dorin Constantin Banu < constatin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-09-22
Issue Date	2026-09-22

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

Two critical vulnerabilities have been disclosed by D-Link affecting DIR-822A routers. Tracked as CVE-2026-86296 and CVE-2026-86510, these vulnerabilities consist of a stack-based buffer overflow in the udhcpcd component and an out-of-bounds write flaw in the L2TP Control Message Parser. Successful exploitation could result in arbitrary code execution, memory corruption, denial-of-service conditions, or compromise of the affected devices.

Risk

Government:

- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:

- Large and medium business entities: **Critical**
- Small business entities: **Critical**

Technical summary

More details related to these vulnerabilities are as follows:

CVE ID	Description
CVE-2026-86296 **CVSS Base Score: 10**	A stack-based buffer overflow vulnerability exists in the `udhcpcd` DHCP server of D-Link DIR-822A. The issue is located in the TR-111 parsing routine for DHCP vendor-specific option 125, where attacker-controlled suboption data is copied into fixed-size stack buffers using `strcpy()` even though the source data is length-delimited DHCP option content rather than a NUL-terminated C string. Because the vulnerable path is reachable from unauthenticated DHCP client traffic on the local network, a remote attacker on the LAN can trigger memory corruption by sending a crafted DHCP message containing a malicious option 125 payload.
CVE-2026-86510 **CVSS Base Score: 9.4**	An out-of-bounds write vulnerability exists in the L2TP control message parser of D-Link DIR-822A. When the device is configured to use L2TP or L2TPv6 WAN connectivity, a malicious upstream L2TP server or an attacker able to spoof or intercept the remote peer can send a crafted control packet containing an oversized Host Name AVP and trigger memory corruption during tunnel setup. The bug affects both the IPv4 and IPv6 L2TP parser variants shipped in the DIR-822A GPL source tree.

Affected Products

Product	Affected Version
D-Link DIR-822A router	Firmware version A_101

Recommendations

Smarttech247 team recommend the following actions be taken:

- Inventory all D-Link DIR-822A devices and identify systems running firmware version A_101
- Ensure affected devices are not unnecessarily exposed to the Internet, particularly administrative interfaces.
- Disable or restrict remote management services unless operationally required.
- Use firewall and network access controls to permit administration only from trusted systems.
- Monitor D-Link's applicable regional support portal for security advisories, firmware updates, and lifecycle guidance.
- Apply the appropriate patches or mitigations to vulnerable systems as soon as they become available from D-Link, following appropriate testing.

References

https://cybersecuritynews.com/d-link-router-hit-by-cvss-10-0-flaw/amp/
https://tzh00203.notion.site/D-Link-DIR-822A-Stack-Overflow-in-udhcpd-TR-111-Option-125-Parsing-33cb5c52018a80238b80e89e7c7c68f0
https://tzh00203.notion.site/D-Link-DIR-822A-L2TP-Host-Name-AVP-Out-of-Bounds-Write-33cb5c52018a80a7af5fdc1af3d5aa73

CVE

CVE-2026-86296
CVE-2026-86510

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com