

CVE-2024-0769

D-Link DIR-859 Router Path Traversal Vulnerability

CISA KEV since Jun 25, 2025

Actively exploited

**** UNSUPPORTED WHEN ASSIGNED **** A vulnerability was found in D-Link DIR-859 1.06B01. It has been rated as critical. Affected by this issue is some unknown functionality of the file /hedwig.cgi of the component HTTP POST Request Handler. The manipulation of the argument service with the input ../../../../htdocs/webinc/getcfg/DHCPS6.BRIDGE-1.xml leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.

EVRs

83/100

Urgent priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.827

99.67th percentile · FIRST

CISA DEADLINE

Jul 16, 2025

KEV since 2025 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.827 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

VDB-251666 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
dir-859 firmware	1.06	no fixed version listed	NVD
dir-859	—	no fixed version listed	NVD

Sources

Vendor guidance	supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10371	NVD	nvd.nist.gov/vuln/detail/CVE-2024-0769
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-16557
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-0769		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.