

CVE-2021-40655

D-Link DIR-605 Router Information Disclosure Vulnerability

CISA KEV since May 16, 2024

Actively exploited

An information disclosure issue exists in D-LINK-DIR-605 B2 Firmware Version : 2.01MT. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page

EVRS 80 / ₁₀₀ Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.867 99.74th percentile · FIRST	CISA DEADLINE Jun 6, 2024 KEV since 2024 · 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	On the CISA KEV catalog for over two years
☒ EPSS	0.867 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: This vulnerability affects legacy D-Link products. All associated hardware revisions have reached their end-of-life (EOL) or end-of-service (EOS) life cycle and should be retired and replaced per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
dir-605l firmware	2.01mt	no fixed version listed	NVD
dir-605l	b2	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-95fh-63xw-wfh3	Additional guidance	dlink.com/en/security-bulletin/nvd.nist.gov/vuln/detail/CVE-2021-40655
legacy.us.dlink.com	legacy.us.dlink.com/pages/product.aspx?id=2b09e95d90ff4cb38830ecc04c89cee5	NVD	
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-27829
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-40655		

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