

CVE-2020-25078

D-Link DCS-2530L and DCS-2670L Devices Unspecified Vulnerability

CISA KEV since Aug 5, 2025

Actively exploited

An issue was discovered on D-Link DCS-2530L before 1.06.01 Hotfix and DCS-2670L through 2.02 devices. The unauthenticated /config/getuser endpoint allows for remote administrator password disclosure.

EVRS 84/₁₀₀ Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.975 99.9th percentile · FIRST	CISA DEADLINE Aug 26, 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	0.975 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: 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

Affected and fixed versions · 10 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
dcx-4603 firmware	< 1.04.02	1.04.02	NVD
dcx-4622 firmware	< 2.01.10	2.01.10	NVD
dcx-4701e firmware	< 2.03.01	2.03.01	NVD
dcx-4703e firmware	< 1.03.04	1.03.04	NVD
dcx-4705e firmware	< 1.03.02	1.03.02	NVD
dcx-4802e firmware	< 2.01.01	2.01.01	NVD
dcx-p703 firmware	—	no fixed version listed	NVD
dcx-2530l firmware	≤ 1.05.05	no fixed version listed	NVD

Sources

Vendor guidance supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10180

NVD nvd.nist.gov/vuln/detail/CVE-2020-25078

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2020-17770

support.dlink.com support.dlink.com/productinfo.aspx?m=DCS-2530L

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2020-25078

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