

CVE-2016-20017

D-Link DSL-2750B Devices Command Injection Vulnerability

CISA KEV since Jan 8, 2024

Actively exploited

Public exploit module (Metasploit)

D-Link DSL-2750B devices before 1.05 allow remote unauthenticated command injection via the login.cgi cli parameter, as exploited in the wild in 2016 through 2022.

EVRS 78/₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.666 99.29th percentile · FIRST	CISA DEADLINE Jan 29, 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	0.666 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 or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
dsl-2750b firmware	< 1.05	1.05	NVD
dsl-2750b	—	no fixed version listed	NVD

Sources

Vendor guidance	supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10088	NVD	nvd.nist.gov/vuln/detail/CVE-2016-20017
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2016-3105
Current data	evulnable.com/vulnerability-management/cve/CVE-2016-20017		

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