D-Link DSL-2750B Devices Command Injection Vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-20017
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-19 05:15:00 UTC
Updated	2024-01-09 02:00:00 UTC
Description	D-Link DSL-2750B devices before 1.05 allow remote unauthenticated command injection via the login.cgi cli parameter, as

Risk And Classification

EPSS: 0.920910000 probability, percentile 0.997170000 (date 2026-05-11)

CISA KEV: Listed on 2024-01-08; due 2024-01-29; ransomware use Unknown

Problem Types: CWE-77

CISA Known Exploited Vulnerability

Vendor	D-Link
Product	DSL-2750B Devices
Name	D-Link DSL-2750B Devices Command Injection Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10088; https://nvd.nist.gov/vuln/detail/CVE-2016-20017

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Dlink	Dsl-2750b	-	All	All	All
Operating System	Dlink	Dsl-2750b Firmware	All	All	All	All

References

Reference	Source	Link
Full Disclosure: D-Link router DSL-2750B firmware 1.01 to 1.03 - remote command execution no auth required	MISC	seclists.org
D-Link Technical Support	MISC	supportannoun

D-Link Technical Support	MISC	supportannoun
D-Link DSL-2750B - OS Command Injection (Metasploit)	MISC	www.exploit-db
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**