D-Link DIR-820 Router OS Command Injection Vulnerability

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

Summary

CVE	CVE-2023-25280
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-16 01:15:00 UTC
Updated	2023-03-21 17:33:00 UTC
Description	OS Command injection vulnerability in D-Link DIR820LA1_FW105B03 allows attackers to escalate privileges to root via a c

Risk And Classification

EPSS: 0.931120000 probability, percentile 0.997950000 (date 2026-05-12)

CISA KEV: Listed on 2024-09-30; due 2024-10-21; ransomware use Unknown

Problem Types: CWE-78

CISA Known Exploited Vulnerability

Vendor	D-Link
Product	DIR-820 Router
Name	D-Link DIR-820 Router OS Command Injection Vulnerability
Required Action	The impacted product is end-of-life (EoL) and/or end-of-service (EoS). Users should discontinue utilization of the product.
Notes	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10358 ; https://nvd.nist.gov/vuln/detail/CVE-2023-25280

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Dlink	Dir820la1	-	All	All	All
Operating System	Dlink	Dir820la1 Firmware	105b03	All	All	All

References

Reference	Source	Link	Tags
D_Link_Vuln/cmd Inject in pingV4Msg at main · migraine-sudo/D_Link_Vuln · GitHub	MISC	github.com	

Security Bulletin | D-Link	MISC	www.dlink.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

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