CVE-2019-20500

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

Summary

CVE	CVE-2019-20500
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-05 15:15:00 UTC
Updated	2023-04-26 19:27:00 UTC
Description	D-Link DWL-2600AP 4.2.0.15 Rev A devices have an authenticated OS command injection vulnerability via the Save Confi

Risk And Classification

EPSS: 0.924530000 probability, percentile 0.997340000 (date 2026-04-20)

CISA KEV: Listed on 2023-06-29; due 2023-07-20; ransomware use Unknown

Problem Types: CWE-78

CISA Known Exploited Vulnerability

Vendor	D-Link
Product	DWL-2600AP Access Point
Name	D-Link DWL-2600AP Access Point Command Injection Vulnerability
Required Action	Apply updates per vendor instructions or discontinue use of the product if updates are unavailable.
Notes	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10113; https://nvd.nist.gov/vuln/detail/CVE-2019-20500

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	D-link	Dwl-2600ap	-	All	All	All
Hardware	D-link	Dwl-2600ap	-	All	All	All
Operating System	D-link	Dwl-2600ap Firmware	All	All	All	All
Hardware	Dlink	Dwl-2600ap	-	All	All	All
Operating System	Dlink	Dwl-2600ap Firmware	All	All	All	All

References

Reference	Source	Link	Tags

Reference	Source	Link	Tags
D-Link DWL-2600AP - Multiple OS Command Injection	MISC	www.exploit-db.com	Exploit, Third Party Advisory, VD
D-Link Technical Support	MISC	supportannouncement.us.dlink.com	Patch, Vendor Advisory
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.

Free CVE JSON API cve.report/api

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