



CVE-2023-0127

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-0127
State	PUBLIC
Assigner	vulnreport@tenable.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-11 18:15:00 UTC
Updated	2023-04-26 19:27:00 UTC
Description	A command injection vulnerability in the firmware_update command, in the device's restricted telnet interface, allows an aut

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	D-link	Dwl-2600ap	-	All	All	All
Operating System	D-link	Dwl-2600ap Firmware	4.2.0.17	All	All	All
Hardware	Dlink	Dwl-2600ap	-	All	All	All
Operating System	Dlink	Dwl-2600ap Firmware	4.2.0.17	All	All	All

References

Reference	Source	Link	Tags
Command Injection in D-Link DWL-2600AP with firmware v4.2.0.17 - Research Advisory Tenable®	MISC	www.tenable.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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