D-Link DIR-600L A1 Hardcoded Telnet Backdoor Credentials

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

Summary

CVE	CVE-2026-42375
State	PUBLISHED
Assigner	securin
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 17:16:25 UTC
Updated	2026-05-06 12:17:37 UTC
Description	D-Link DIR-600L Hardware Revision A1 (End-of-Life) contains a hardcoded telnet backdoor. The device starts a telnet daer

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000610000 probability, percentile 0.188450000 (date 2026-05-05)

Problem Types: CWE-798 | CWE-798 CWE-798 Use of Hard-coded Credentials

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	33c584b5-0579-4c06-b2a0-8d8329fcab9c	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Dlink	Dir-600l	a1	All	All	All
Operating System	Dlink	Dir-600l Firmware	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	D-Link	DIR-600L Firmware	affected A1 custom	MIPS32 Big-Endian

References

Reference	Source	Link
www.securin.io/zero-day/cve-2026-42375-hardcoded-telnet-backdoor-in-d-link-d...	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.securin
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Arjun Basnet from Securin Labs (en)

Additional Advisory Data

Workarounds

CNA: This product is End-of-Life and will NOT receive patches. Users should replace the device. Temporary: connect via backdoor and run "killall telnetd" and "iptables -A INPUT -p tcp --dport 23 -j DROP" (lost on reboot).

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