



# D-Link DIR-456U A1 Hardcoded Telnet Backdoor Credentials

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

## Summary

<b>CVE</b>	CVE-2026-42376
<b>State</b>	PUBLISHED
<b>Assigner</b>	securin
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-04 17:16:26 UTC
<b>Updated</b>	2026-05-05 19:32:23 UTC
<b>Description</b>	D-Link DIR-456U Hardware Revision A1 (End-of-Life, EOL) contains a hardcoded telnet backdoor. The device starts a telnet

## Risk And Classification

**Primary CVSS:** v3.1 9.8 CRITICAL from 33c584b5-0579-4c06-b2a0-8d8329fcab9c

**CVSS:** 3.1/AV:N/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	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

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	D-Link	DIR-456U Firmware	affected A1 custom	MIPS32 Little-Endian

#### References

Reference	Source	Link
<a href="http://www.securin.io/zero-day/cve-2026-42376-hardcoded-telnet-backdoor-in-d-link-d...">www.securin.io/zero-day/cve-2026-42376-hardcoded-telnet-backdoor-in-d-link-d...</a>	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="http://www.securin.io">www.securin.io</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

#### Vendor Comments And Credit

Discovery Credit

**CNA:** Arjun Basnet from Securin Labs (en)

#### Additional Advisory Data

Workarounds

**CNA:** This product is End-of-Life (EOL) 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.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)