



# CVE-2020-25078

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

## Summary

<b>CVE</b>	CVE-2020-25078
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-09-02 16:15:00 UTC
<b>Updated</b>	2023-11-08 22:50:00 UTC
<b>Description</b>	An issue was discovered on D-Link DCS-2530L before 1.06.01 Hotfix and DCS-2670L through 2.02 devices. The unauthen

## Risk And Classification

**EPSS:** 0.941460000 probability, percentile 0.999130000 (date 2026-04-01)

**CISA KEV:** Listed on 2025-08-05; due 2025-08-26; ransomware use Unknown

**Problem Types:** NVD-CWE-noinfo

## CISA Known Exploited Vulnerability

<b>Vendor</b>	D-Link
<b>Product</b>	DCS-2530L and DCS-2670L Devices
<b>Name</b>	D-Link DCS-2530L and DCS-2670L Devices Unspecified Vulnerability
<b>Required Action</b>	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
<b>Notes</b>	<a href="https://support.dlink.com/productinfo.aspx?m=DCS-2530L">https://support.dlink.com/productinfo.aspx?m=DCS-2530L</a> ; <a href="https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10180">https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10180</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2020-25078">https://nvd.nist.gov/vuln/detail/CVE-2020-25078</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">D-link</a>	<a href="#">Dcs-2530l</a>	-	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dcs-2530l</a>	-	All	All	All
Operating System	<a href="#">D-link</a>	<a href="#">Dcs-2530l Firmware</a>	All	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dcs-2670l</a>	-	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dcs-2670l</a>	-	All	All	All
Operating System	<a href="#">D-link</a>	<a href="#">Dcs-2670l Firmware</a>	All	All	All	All

Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-2530l</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-2530l Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-2670l</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-2670l Firmware</a>	All	All	All	All

## References

### Reference

Kaff on Twitter: "Well done Dlink. DCS-2530L unauthenticated admin password reveal. Wasn't an exciting find - just disappointing. Pair with pr

[D-Link Technical Support](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

[CISA Known Exploited Vulnerabilities catalog](#)

No vendor comments have been submitted for this CVE.

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)