Posted Date: 2025/08/12

[Vulnerability Alert] CISA Adds 3 New Vulnerabilities to KEV Catalog (2025/08/04-2025/08/10)

* Subject: [Vulnerability Alert] CISA Adds 3 New Vulnerabilities to KEV Catalog (2025/08/04-2025/08/10)

* Content:

- Forwarded from TWCERTCC-200-202508-00000006, Taiwan Computer Emergency Response Team/Coordination Center

1. [CVE-2020-25078] D-Link DCS-2530L and DCS-2670L Devices Unspecified Vulnerability (CVSS v3.1: 7.5)
    - [Exploited by Ransomware: Unknown] An unspecified vulnerability exists in D-Link DCS-2530L and DCS-2670L devices that may lead to remote administrator password leakage.
    - [Affected Platforms] Please refer to the official list of affected versions.
    - https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10180
2. [CVE-2020-25079] D-Link DCS-2530L and DCS-2670L Command Injection Vulnerability (CVSS v3.1: 8.8)
    - [Exploited by Ransomware: Unknown] A command injection vulnerability exists in D-Link DCS-2530L and DCS-2670L devices in cgi-bin/ddns_enc.cgi.
    - [Affected Platforms] Please refer to the official list of affected versions.
    - https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10180
3. [CVE-2022-40799] D-Link DNR-322L Download of Code Without Integrity Check Vulnerability (CVSS v3.1: 8.8)
    - [Exploited by Ransomware: Unknown] D-Link DNR-322L has a vulnerability in downloading code without an integrity check, which may allow an authenticated attacker to execute operating system-level commands on the device.
    - [Affected Platforms] D-Link DNR-322L versions prior to and including 2.60B15.

* Affected Platforms:

- Details are in the Affected Platforms section of the Content description.

* Recommended Measures:

1. [CVE-2020-25078]
    - The affected products may have reached End of Life (EoL) and/or End of Service (EoS). Users are advised to stop using these products.
2. [CVE-2020-25079]
    - The affected products may have reached End of Life (EoL) and/or End of Service (EoS). Users are advised to stop using these products.

3. [CVE-2022-40799]
    - The affected products may have reached End of Life (EoL) and/or End of Service (EoS). Users are advised to stop using these products.

Computer and Communications Center
Network Systems Division Respectfully

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250812_02

Last update: **2025/08/12 15:07**