

張貼日期: 2025/08/12

【漏洞預警】CISA新增3個已知遭駭客利用之漏洞至KEV目錄 (2025/08/04-2025/08/10)

- 主旨說明: 【漏洞預警】CISA新增3個已知遭駭客利用之漏洞至KEV目錄 (2025/08/04-2025/08/10)

- 內容說明:

- 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202508-00000006

- 1. CVE-2020-25078 D-Link DCS-2530L and DCS-2670L Devices Unspecified Vulnerability (CVSS v3.1: 7.5)
 - 【是否遭勒索軟體利用】未知 D-Link DCS-2530L和DCS-2670L裝置存在一個未具體說明的漏洞，可能導致遠端管理員密碼洩露。
 - 【影響平台】請參考官方所列的影響版本
 - <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)
 - 【是否遭勒索軟體利用】未知 D-Link DCS-2530L和DCS-2670L裝置在cgi-bin/ddns_enc.cgi存在指令注入漏洞。
 - 【影響平台】請參考官方所列的影響版本
 - <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)
 - 【是否遭勒索軟體利用】未知 D-Link DNR-322L存在下載程式碼時未進行完整性檢查漏洞，可能允許已驗證的攻擊者在裝置上執行作業系統層級的指令。
 - 【影響平台】D-Link DNR-322L 2.60B15(含)之前的版本

- 影響平台:

- 詳細內容於內容說明欄之影響平台

- 建議措施:

- 1. CVE-2020-25078
 - 受影響的產品可能已達到產品生命週期終點【EoL】和/或終止服務【EoS】，建議使用者停止使用這些產品。

- 2. CVE-2020-25079
 - 受影響的產品可能已達到產品生命週期終點【EoL】和/或終止服務【EoS】，建議使用者停止使用這些產品。

- 3. CVE-2022-40799
 - 受影響的產品可能已達到產品生命週期終點【EoL】和/或終止服務【EoS】，建議使用者停止使用這些產品。

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

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

Last update: **2025/08/12 15:06**