

ANA事件單通知:TACERT-ANA-2025081201081515【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)

教育機構ANA通報平台

發佈編號	TACERT-ANA-2025081201081515	發佈時間	2025-08-12 13:54:16
事故類型	ANA-漏洞預警	發現時間	2025-08-12 13:54:16
影響等級	低		
[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			

情資分享等級：WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助轉發與通知轄下各單位知悉

[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。

[參考資料:]

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組

網址：<https://info.cert.tanet.edu.tw/>

專線電話：07-5250211

網路電話：98400000

E-Mail：service@cert.tanet.edu.tw