張貼日期：2026/05/21

【漏洞預警】CISA新增2個已知遭駭客利用之漏洞至KEV目錄(2026/05/11-2026/05/17)

- 主旨說明:【漏洞預警】CISA新增2個已知遭駭客利用之漏洞至KEV目錄(2026/05/11-2026/05/17)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-200-202605-00000012
  - 【CVE-2026-20182】Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability (CVSS v3.1: 10.0)
  - 【是否遭勒索軟體利用:未知】 Cisco Catalyst SD-WAN Controller & Manager 存在身份驗證繞過漏洞，未經驗證的遠端攻擊者可藉此繞過身份驗證，並在受影響的系統上取得管理員權限。
  - 【CVE-2026-42897】Microsoft Exchange Server Cross-Site Scripting Vulnerability (CVSS v3.1: 8.1)
  - 【是否遭勒索軟體利用:未知】 Microsoft Exchange Server 在 Outlook Web Access 產生網頁時存在跨網站指令碼漏洞；在特定互動條件下，攻擊者可在瀏覽器環境中執行任意 JavaScript 程式碼。
- 影響平台:
  - 【CVE-2026-20182】請參考官方所列的影響版本 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW
  - 【CVE-2026-42897】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897
- 建議措施:
  - 【CVE-2026-20182】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW
  - 【CVE-2026-42897】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897

計算機與通訊中心
網路系統組 敬啟