張貼日期：2026/06/30

【漏洞預警】CISA新增6個已知遭駭客利用之漏洞至KEV目錄(2026/06/22-2026/06/28)

- 主旨說明:【漏洞預警】CISA新增6個已知遭駭客利用之漏洞至KEV目錄(2026/06/22-2026/06/28)

- 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-200-202606-00000018
  - 【CVE-2025-67038】Lantronix EDS5000 Code Injection Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 Lantronix EDS5000 存在程式碼注入漏洞，攻擊者可利用此漏洞將任意作業系統指令注入至 username 參數並以 root 權限執行。
  - 【CVE-2026-34910】Ubiquiti UniFi OS Improper Input Validation Vulnerability (CVSS v3.1: 10.0)
  - 【是否遭勒索軟體利用:未知】 Ubiquiti UniFi OS 存在不當輸入驗證漏洞，具備網路存取權限的惡意攻擊者可利用此漏洞執行指令注入攻擊。
  - 【CVE-2026-34909】Ubiquiti UniFi OS Path Traversal Vulnerability (CVSS v3.1: 10.0)
  - 【是否遭勒索軟體利用:未知】 Ubiquiti UniFi OS 存在路徑遍歷漏洞，具備網路存取權限的惡意攻擊者可利用此漏洞存取底層系統上的檔案，並可能藉由操控或利用這些檔案，進一步取得底層系統帳戶的存取權限。
  - 【CVE-2026-34908】Ubiquiti UniFi OS Improper Access Control Vulnerability (CVSS v3.1: 10.0)
  - 【是否遭勒索軟體利用:未知】 Ubiquiti UniFi OS 存在不當存取控制漏洞，具備網路存取權限的惡意攻擊者可利用此漏洞對系統進行未經授權的變更。
  - 【CVE-2026-12569】PTC Windchill and FlexPLM Improper Input Validation Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 PTC Windchill 與 FlexPLM 存在不當輸入驗證漏洞，未經驗證的遠端攻擊者可透過向網路發送惡意請求來執行任意程式碼。
  - 【CVE-2026-20230】Cisco Unified Communications Manager Server-Side Request Forgery (SSRF) Vulnerability (CVSS v3.1: 8.6)
  - 【是否遭勒索軟體利用:未知】 Cisco Unified Communications Manager【Unified CM】 與 Cisco Unified Communications Manager Session Management Edition【Unified CM SME】 存在伺服器端請求偽造漏洞，未經驗證的遠端攻擊者可利用此漏洞將檔案寫入底層作業系統，並於後續利用這些檔案進一步提升權限至 root【
- 影響平台:
  - 【CVE-2025-67038】請參考官方所列的影響版本 https://www.lantronix.com/technical-support/security-updates/vulnerability-disclosure-policy/vulnerability-library/cve-2025-67038-eds-5000-eds-3000/?_gl=1*11k48gn*_up*MQ..*_ga*NzY1MzgwNjcxLjE3ODI2OTc0Nzg.*_ga_M2G6RLT5L3*czE3ODI2OTc0NzckbzEkZzEkdDE3ODI2OTc1NTckajYwJGwwJGgw
  - 【CVE-2026-34910】請參考官方所列的影響版本 https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
  - 【CVE-2026-34909】請參考官方所列的影響版本 https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
  - 【CVE-2026-34908】請參考官方所列的影響版本 https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42a

b-bd61-cc994445963b
    - CVE-2026-12569請參考官方所列的影響版本
      https://www.ptc.com/en/support/article/CS473270
    - CVE-2026-20230請參考官方所列的影響版本
      https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssrf-cXPnHcW
- 建議措施:
    - CVE-2025-67038 官方已針對漏洞釋出修復更新，請更新至相關版本
      https://www.lantronix.com/technical-support/security-updates/vulnerability-disclosure-policy/vulnerability-library/cve-2025-67038-eds-5000-eds-3000/?_gl=1*11k48gn*_up*MQ..*_ga*NzY1MzgwNjcxLjE3ODI2OTc0Nzg.*_ga_M2G6RLT5L3*czE3ODI2OTc0NzckbzEkZzEkdDE3ODI2OTc1NTckajYwJGwwJGgw
    - CVE-2026-34910 官方已針對漏洞釋出修復更新，請更新至相關版本
      https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
    - CVE-2026-34909 官方已針對漏洞釋出修復更新，請更新至相關版本
      https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
    - CVE-2026-34908 官方已針對漏洞釋出修復更新，請更新至相關版本
      https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
    - CVE-2026-12569 官方已針對漏洞釋出修復更新，請更新至相關版本
      https://www.ptc.com/en/support/article/CS473270
    - CVE-2026-20230 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-cucm-ssrf-cXPnHcW

計算機與通訊中心
網路系統組 敬啟