張貼日期：2026/06/04

【漏洞預警】CISA新增5個已知遭駭客利用之漏洞至KEV目錄(2026/05/25-2026/05/31)

- 主旨說明:【漏洞預警】CISA新增5個已知遭駭客利用之漏洞至KEV目錄(2026/05/25-2026/05/31)

- 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-200-202606-00000001
  - 【CVE-2026-48172】LiteSpeed cPanel Plugin Privilege Escalation Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 LiteSpeed cPanel Plugin 存在權限提升漏洞。該漏洞可經由使用者端的 cPanel 外掛程式觸發，任何 cPanel 使用者帳號都可能濫用此漏洞，以 root權限執行任意指令碼。
  - 【CVE-2026-48027】Nx Console Embedded Malicious Code Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:已知】 Nx Console 存在嵌入式惡意程式碼漏洞。攻擊者藉此發布惡意版本的 Nx Console【受影響的擴充套件會下載經過混淆處理的惡意載荷，可從磁碟與記憶體中的多個來源竊取憑證。
  - 【CVE-2026-45321】TanStack Unspecified Vulnerability (CVSS v31: 9.6)
  - 【是否遭勒索軟體利用:已知】 TanStack 存在未具體說明的漏洞，使攻擊者得以將惡意版本的套件發布至 npm Registry【並利用受信任的身分發布竊取憑證的惡意軟體。
  - 【CVE-2026-8398】Daemon Tools Lite Embedded Malicious Code Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 Daemon Tools 存在未具體說明的漏洞，對機密性、完整性及可用性造成高度影響。
  - 【CVE-2026-0257】Palo Alto Networks PAN-OS Authentication Bypass Vulnerability (CVSS v3.1: 9.1)
  - 【是否遭勒索軟體利用:未知】 Palo Alto Networks PAN-OS 存在身分驗證繞過漏洞，攻擊者可藉此繞過安全限制並建立未經授權的 VPN 連線。
- 影響平台:
  - 【CVE-2026-48172】請參考官方所列的影響版本 https://blog.litespeedtech.com/2026/05/21/security-update-for-litespeed-cpanel-plugin/
  - 【CVE-2026-48027】請參考官方所列的影響版本 https://nx.dev/blog/nx-console-v18-95-0-postmortem#indicators-of-compromise
  - 【CVE-2026-45321】請參考官方所列的影響版本 https://github.com/TanStack/router/security/advisories/GHSA-g7cv-rxg3-hmpx
  - 【CVE-2026-8398】請參考官方所列的影響版本 https://blog.daemon-tools.cc/post/security-incident
  - 【CVE-2026-0257】請參考官方所列的影響版本 https://security.paloaltonetworks.com/CVE-2026-0257
- 建議措施:
  - 【CVE-2026-48172】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://blog.litespeedtech.com/2026/05/21/security-update-for-litespeed-cpanel-plugin/
  - 【CVE-2026-48027】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://nx.dev/blog/nx-console-v18-95-0-postmortem#indicators-of-compromise
  - 【CVE-2026-45321】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://github.com/TanStack/router/security/advisories/GHSA-g7cv-rxg3-hmpx

- 【CVE-2026-8398】 官方已針對漏洞釋出修復更新，請更新至相關版本
  https://blog.daemon-tools.cc/post/security-incident
- 【CVE-2026-0257】 官方已針對漏洞釋出修復更新，請更新至相關版本
  https://security.paloaltonetworks.com/CVE-2026-0257

計算機與通訊中心
網路系統組 敬啟