張貼日期：2026/05/15

【漏洞預警】CISA新增3個已知遭駭客利用之漏洞至KEV目錄(2026/05/04-2026/05/10)

- 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(2026/05/04-2026/05/10)

- 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-200-202605-00000010
  - 【CVE-2026-0300】Palo Alto Networks PAN-OS Out-of-bounds Write Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 Palo Alto Networks 的 PAN-OS 在 User-ID Authentication Portal 服務中存在越界寫入漏洞。未經驗證的攻擊者可透過傳送特製封包，在 PA-Series 與 VM-Series 防火牆上以 root 權限執行任意程式碼。
  - 【CVE-2026-6973】Ivanti Endpoint Manager Mobile (EPMM) Improper Input Validation Vulnerability (CVSS v3.1: 7.2)
  - 【是否遭勒索軟體利用:未知】 Ivanti Endpoint Manager Mobile【EPMM】存在不當輸入驗證漏洞，具管理員權限的遠端已驗證使用者可利用此漏洞達成遠端程式碼執行。
  - 【CVE-2026-42208】BerriAI LiteLLM SQL Injection Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 BerriAI LiteLLM 存在 SQL 注入漏洞，攻擊者可利用此漏洞從代理伺服器的資料庫讀取資料，並可能進行竄改，導致未經授權存取該代理伺服器及其所管理的憑證。
- 影響平台:
  - 【CVE-2026-0300】請參考官方所列的影響版本 https://security.paloaltonetworks.com/CVE-2026-0300
  - 【CVE-2026-6973】請參考官方所列的影響版本 https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs
  - 【CVE-2026-42208】請參考官方所列的影響版本 https://github.com/BerriAI/litellm/security/advisories/GHSA-r75f-5x8p-qvmc
- 建議措施:
  - 【CVE-2026-0300】 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-2026-0300
  - 【CVE-2026-6973】 官方已針對漏洞釋出修復更新，請更新至相關版本
  - https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs
  - 【CVE-2026-42208】 官方已針對漏洞釋出修復更新，請更新至相關版本
  - https://github.com/BerriAI/litellm/security/advisories/GHSA-r75f-5x8p-qvmc

---

計算機與通訊中心
網路系統組 敬啟

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

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20260515_25

Last update: **2026/05/15 10:28**