張貼日期：2026/07/28

【漏洞預警】CISA新增6個已知遭駭客利用之漏洞至KEV目錄(2026/07/20-2026/07/26)

- 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(2026/07/20-2026/07/26)

- 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-200-202607-00000012
  - 【CVE-2026-60137】WordPress Core SQL Injection Vulnerability (CVSS v3.1: 5.9)
  - 【是否遭勒索軟體利用:未知】 WordPress Core在外掛或佈景主題將不可信任的輸入傳遞至該參數時，存在SQL注入漏洞。此漏洞可與 CVE-2026-63030 串聯利用，使未經驗證的攻擊者得以在預設的WordPress安裝環境中取得遠端程式碼執行權限。
  - 【CVE-2026-63030】WordPress Core Interpretation Conflict Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 WordPress Core存在Interpretation Conflict漏洞，可能允許攻擊者執行SQL注入並實現遠端程式碼執行。此漏洞可與CVE-2026-60137串聯利用。
  - 【CVE-2026-0770】Langflow Inclusion of Functionality from Untrusted Control Sphere Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 Langflow存在Inclusion of Functionality from Untrusted Control Sphere漏洞，允許遠端攻擊者在受影響的安裝環境中執行任意程式碼。
  - 【CVE-2021-27137】DD-WRT Stack-Based Buffer Overflow Vulnerability (CVSS v3.1: 8.1)
  - 【是否遭勒索軟體利用:未知】 DD-WRT存在堆疊型緩衝區溢位漏洞，未經驗證的攻擊者可利用此漏洞使UPnP使用的內部緩衝區發生溢位，進而觸發程式碼執行漏洞。
  - 【CVE-2026-16232】Check Point SmartConsole Improper Authentication Vulnerability (CVSS v3.1: 9.1)
  - 【是否遭勒索軟體利用:未知】 Check Point SmartConsole存在不當驗證漏洞，未經驗證的遠端攻擊者可利用此漏洞取得應用程式的登入權杖，並藉此以完整管理員權限進行驗證。
  - 【CVE-2026-50522】Microsoft SharePoint Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 Microsoft SharePoint存在反序列化不受信任資料漏洞，未經授權的攻擊者可能利用此漏洞透過網路執行任意程式碼。
- 影響平台:
  - 【CVE-2026-60137】請參考官方所列的影響版本 https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-fpp7-x2x2-2mjf
  - 【CVE-2026-63030】請參考官方所列的影響版本 https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-ff9f-jf42-662q
  - 【CVE-2026-0770】 Langflow 1.7.3(含)之前的版本
  - 【CVE-2021-27137】 DD-WRT 45724之前的版本
  - 【CVE-2026-16232】請參考官方所列的影響版本 https://support.checkpoint.com/results/sk/sk185169/
  - 【CVE-2026-50522】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50522
- 建議措施:
  - 【CVE-2026-60137】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-fpp7-x2x2-2mjf

- CVE-2026-63030 官方已針對漏洞釋出修復更新，請更新至相關版本
  https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-ff9f-jf42-662q
- CVE-2026-0770 目前官方尚未釋出對應修補程式，建議更新至其他未受影響版本
  https://github.com/langflow-ai/langflow
- CVE-2021-27137 官方已針對漏洞釋出修復更新，請更新至相關版本
  https://svn.dd-wrt.com/changeset/45724
- CVE-2026-16232 官方已針對漏洞釋出修復更新，請更新至相關版本
  https://support.checkpoint.com/results/sk/sk185169/
- CVE-2026-50522 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-2026-50522

計算機與通訊中心
網路系統組 敬啟