張貼日期：2025/09/12

【漏洞預警】CISA新增7個已知遭駭客利用之漏洞至KEV目錄(2025/09/01-2025/09/07)

- 主旨說明:【漏洞預警】CISA新增7個已知遭駭客利用之漏洞至KEV目錄(2025/09/01-2025/09/07)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202509-00000004

1. 【CVE-2020-24363】TP-link TL-WA855RE Missing Authentication for Critical Function Vulnerability (CVSS v3.1: 8.8)
   - 【是否遭勒索軟體利用:未知】 TP-Link TL-WA855RE 存在關鍵功能未進行適當驗證的漏洞。未經身份驗證的攻擊者若與裝置位於同一網路，可能透過提交 TDDP_RESET POST 請求，強制設備回復出廠設定並重新啟動。攻擊者隨後可設定新的管理員密碼，進而取得未經授權的存取控制權限。受影響的產品可能已達產品生命週期結束(EoL)和／或終止產品支援(EoS)，建議使用者停止使用該產品。
   - 【影響平台】 TP-Link TL-WA855RE V5 200731之前的版本
2. 【CVE-2025-55177】Meta Platforms WhatsApp Incorrect Authorization Vulnerability (CVSS v3.1: 5.4)
   - 【是否遭勒索軟體利用:未知】 Meta Platforms 的 WhatsApp 存在授權錯誤漏洞，起因於對已連結裝置同步訊息的授權檢查不完整。此漏洞可能使無關使用者得以在目標裝置上觸發並處理任意 URL 的內容。
   - 【影響平台】請參考官方所列的影響版本
   - https://www.facebook.com/security/advisories/cve-2025-55177
3. 【CVE-2023-50224】TP-Link TL-WR841N Authentication Bypass by Spoofing Vulnerability (CVSS v3.1: 6.5)
   - 【是否遭勒索軟體利用:未知】 TP-Link TL-WR841N 存在可藉由偽造方式繞過身份驗證的漏洞，該漏洞位於 httpd 服務(預設監聽 TCP 埠 80)，可能導致已儲存的憑證資訊外洩。受影響的產品可能已達產品生命週期終點(EoL)和／或服務終止(EoS)，建議使用者停止使用該產品。
   - 【影響平台】 TP-Link TL-WR841N V12
4. 【CVE-2025-9377】TP-Link Archer C7(EU) and TL-WR841N/ND(MS) OS Command Injection Vulnerability (CVSS v3.1: 7.2)
   - 【是否遭勒索軟體利用:未知】 TP-Link Archer C7(EU)及 TL-WR841N/ND(MS)存在作業系統指令注入漏洞，該漏洞位於家長控制頁面。受影響的產品可能已達產品生命週期結束(EoL)和／或終止產品支援(EoS)，建議使用者停止使用該產品。
   - 【影響平台】
   - TP-Link TL-WR841N/ND(MS) V9 241108之前的版本
   - TP-Link Archer C7(EU) V2 241108之前的版本
5. 【CVE-2025-38352】Linux Kernel Time-of-Check Time-of-Use (TOCTOU) Race Condition Vulnerability (CVSS v3.1: 7.4)
   - 【是否遭勒索軟體利用:未知】 Linux 核心存在TOCTOU競爭條件漏洞，對機密性、完整性與可用性造成高度影響。
   - 【影響平台】
   - Linux kernel 2.6.36至5.4.295(不含)的版本
   - Linux kernel 5.5至5.10.239(不含)的版本
   - Linux kernel 5.11至5.15.186(不含)的版本
   - Linux kernel 5.16至6.1.142(不含)的版本

        - Linux kernel 6.2至6.6.94(不含)的版本
        - Linux kernel 6.7至6.12.34(不含)的版本
        - Linux kernel 6.13至6.15.3(不含)的版本
        - Linux kernel 6.16
    6. CVE-2025-48543Android Runtime Use-After-Free Vulnerability (CVSS v3.1: 8.8)
        - 【是否遭勒索軟體利用:未知】 Android Runtime存在記憶體釋放後使用漏洞，可能導致Chrome 沙箱逃逸，進而造成本機權限提升。
        - 【影響平台】請參考官方所列的影響版本
        - https://source.android.com/security/bulletin/2025-09-01
    7. CVE-2025-53690Sitecore Multiple Products Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.0)
        - 【是否遭勒索軟體利用:未知】 Sitecore Experience Manager(XM)Experience Platform(XP)Experience Commerce(XC) 以及Managed Cloud存在未經信任資料反序列化漏洞，與使用預設的machine key有關。此漏洞可能允許攻擊者利用外洩的ASP.NET machine key達成遠端程式碼執行。
        - 【影響平台】請參考官方所列的影響版本
        - https://support.sitecore.com/kb
- 影響平台:
    - 詳細內容於內容說明欄之影響平台
- 建議措施:
    1. CVE-2020-24363 官方已針對漏洞釋出修復更新，請更新至相關版本
        - https://www.tp-link.com/us/support/download/tl-wa855re/v5/#Firmware
    2. CVE-2025-55177 官方已針對漏洞釋出修復更新，請更新至相關版本
        - https://www.facebook.com/security/advisories/cve-2025-55177
    3. CVE-2023-50224 官方已針對漏洞釋出修復更新，請更新至相關版本
        - https://www.tp-link.com/en/support/download/tl-wr841n/v12/#Firmware
    4. CVE-2025-9377 官方已針對漏洞釋出修復更新，請更新至相關版本
        - https://www.tp-link.com/us/support/faq/4308/
    5. CVE-2025-38352 官方已針對漏洞釋出修復更新，請更新至相關版本
        - https://git.kernel.org/stable/c/2c72fe18cc5f9f1750f5bc148cf1c94c29e106ff
        - https://git.kernel.org/stable/c/2f3daa04a9328220de46f0d5c919a6c0073a9f0b
        - https://git.kernel.org/stable/c/460188bc042a3f40f72d34b9f7fc6ee66b0b757b
        - https://git.kernel.org/stable/c/764a7a5dfda23f69919441f2eac2a83e7db6e5bb
        - https://git.kernel.org/stable/c/78a4b8e3795b31dae58762bc091bb0f4f74a2200
        - https://git.kernel.org/stable/c/c076635b3a42771ace7d276de8dc3bc76ee2ba1b
        - https://git.kernel.org/stable/c/c29d5318708e67ac13c1b6fc1007d179fb65b4d7
        - https://git.kernel.org/stable/c/f90fff1e152dedf52b932240ebbd670d83330eca
    6. CVE-2025-48543 官方已針對漏洞釋出修復更新，請更新至相關版本
        - https://source.android.com/security/bulletin/2025-09-01
    7. CVE-2025-53690 官方已針對漏洞釋出修復更新，請更新至相關版本
        - https://support.sitecore.com/kb

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:20250912_01

Last update: **2025/09/12 14:28**