張貼日期：2026/02/06

【漏洞預警】CISA新增7個已知遭駭客利用之漏洞至KEV目錄(2026/01/26-2026/02/01)

- 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(2026/01/26-2026/02/01)

- 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-200-202602-00000001
  - 【CVE-2018-14634】Linux Kernel Integer Overflow Vulnerability (CVSS v3.1: 7.8)
  - 【是否遭勒索軟體利用:未知】 Linux Kernel 中的 create_elf_tables() 函式存在整數溢位漏洞，可能允許具 SUID（或其他特權） 二進位檔存取權限的非特權本機使用者提升權限。
  - 【CVE-2025-52691】SmarterTools SmarterMail Unrestricted Upload of File with Dangerous Type Vulnerability (CVSS v3.1: 10.0)
  - 【是否遭勒索軟體利用:未知】 SmarterTools SmarterMail 存在未受限制的危險類型檔案上傳漏洞，可能允許未經驗證的攻擊者將任意檔案上傳至郵件伺服器上的任何位置，進而可能實現遠端程式碼執行。
  - 【CVE-2026-23760】SmarterTools SmarterMail Authentication Bypass Using an Alternate Path or Channel Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 SmarterTools SmarterMail 在密碼重設 API 中存在身分驗證繞過漏洞【force-reset-password 端點允許匿名請求，且在重設系統管理員帳號時無法驗證既有密碼或重設權杖。未經身分驗證的攻擊者只需提供目標管理員使用者名稱與新密碼，即可重設該帳號，從而導致 SmarterMail 實例被接管。
  - 【CVE-2026-24061】GNU InetUtils Argument Injection Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 GNU InetUtils 的 telnetd 中存在參數注入漏洞，攻擊者可透過將 USER 環境變數設為 【-f root】進而實現遠端身分驗證繞過。
  - 【CVE-2026-21509】Microsoft Office Security Feature Bypass Vulnerability (CVSS v3.1: 7.8)
  - 【是否遭勒索軟體利用:未知】 Microsoft Office 存在安全功能繞過漏洞，該漏洞源於其在安全決策過程中依賴不受信任的輸入，可能使未經授權的攻擊者在本機繞過安全防護機制。部分受影響的產品可能已達生命週期終止【EoL】及／或服務終止【EoS】，建議使用者停止使用，並遷移至仍受支援的版本。
  - 【CVE-2026-24858】Fortinet Multiple Products Authentication Bypass Using an Alternate Path or Channel Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 Fortinet FortiAnalyzer、FortiManager、FortiOS 與 FortiProxy 存在身分驗證繞過漏洞。在受影響裝置啟用 FortiCloud SSO 驗證的情況下，擁有 FortiCloud 帳號且已註冊裝置的攻擊者，可能登入註冊於其他帳號之下的裝置。
  - 【CVE-2026-1281】Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 Ivanti Endpoint Manager Mobile（EPMM） 存在程式碼注入漏洞，可能允許攻擊者在未經身分驗證的情況下實現遠端程式碼執行。
- 影響平台:
  - 【CVE-2018-14634】
  - Linux kernel 2.6.0至2.6.39.4版本
  - Linux kernel 3.10至3.10.102版本
  - Linux kernel 4.14至4.14.54版本
  - 【CVE-2025-52691】
  - SmarterTools SmarterMail Build 9413之前的版本
  - 【CVE-2026-23760】

    - SmarterTools SmarterMail Build 9511之前的版本
    - CVE-2026-24061
    - 請參考官方所列的影響版本 https://lists.gnu.org/archive/html/bug-inetutils/2026-01/msg00004.html
    - CVE-2026-21509
    - 請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509
    - CVE-2026-24858
    - 請參考官方所列的影響版本 https://fortiguard.fortinet.com/psirt/FG-IR-26-060
    - CVE-2026-1281
    - 請參考官方所列的影響版本 https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340
- 建議措施:
    - CVE-2018-14634
    - 系統管理員應向產品供應商查詢其 Linux 作業系統是否受影響。若修補程式已提供，應遵從產品供應商建議，立即採取行動以降低風險。
    - CVE-2025-52691
    - 對應產品升級至以下版本(或更高) SmarterMail Build 9413
    - CVE-2026-23760
    - 對應產品升級至以下版本(或更高) SmarterMail Build 9511
    - CVE-2026-24061
    - 官方已針對漏洞釋出修復更新，請更新至相關版本 https://lists.gnu.org/archive/html/bug-inetutils/2026-01/msg00004.html
    - CVE-2026-21509
    - 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-2026-21509
    - CVE-2026-24858
    - 官方已針對漏洞釋出修復更新，請更新至相關版本 https://fortiguard.fortinet.com/psirt/FG-IR-26-060
    - CVE-2026-1281
    - 官方已針對漏洞釋出修復更新，請更新至相關版本 https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340

計算機與通訊中心
網路系統組 敬啟