張貼日期：2026/03/19

【漏洞預警】CISA新增6個已知遭駭客利用之漏洞至KEV目錄(2026/03/09-2026/03/15)

- 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(2026/03/09-2026/03/15)

- 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-200-202603-00000014
  - 【CVE-2021-22054】Omnissa Workspace ONE Server-Side Request Forgery (CVSS v3.1: 7.5)
  - 【是否遭勒索軟體利用:未知】 Omnissa Workspace ONE UEM 存在伺服器端請求偽造漏洞。
  - 此漏洞可能允許具有 UEM 網路存取權限的惡意攻擊者，在未經驗證的情況下發送請求，並取得敏感資訊。
  - 【CVE-2025-26399】SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 SolarWinds Web Help Desk 的 AjaxProxy 元件存在不受信任資料反序列化漏洞。
  - 此漏洞可能允許攻擊者在主機系統上執行指令。
  - 【CVE-2026-1603】Ivanti Endpoint Manager (EPM) Authentication Bypass Vulnerability (CVSS v3.1: 8.6)
  - 【是否遭勒索軟體利用:未知】 Ivanti Endpoint Manager【EPM】存在身分驗證繞過漏洞。
  - 此漏洞可能允許遠端未經驗證的攻擊者洩漏特定的儲存憑證資料。
  - 【CVE-2025-68613】n8n Improper Control of Dynamically-Managed Code Resources Vulnerability (CVSS v3.1: 9.9)
  - 【是否遭勒索軟體利用:未知】 n8n 的workflow expression evaluation system中存在對動態管理程式碼資源控制不當的漏洞，可能導致遠端程式碼執行。
  - 【CVE-2026-3910】Google Chromium V8 Improper Restriction of Operations Within the Bounds of a Memory Buffer Vulnerability (CVSS v3.1: 8.8)
  - 【是否遭勒索軟體利用:未知】 Google Chromium V8 存在記憶體緩衝區內操作限制不當的漏洞，可能允許遠端攻擊者透過特製的 HTML 頁面在沙箱內執行任意程式碼。
  - 此漏洞可能影響多個使用 Chromium 的網頁瀏覽器，包括但不限於 Google Chrome【Microsoft Edge 及 Opera】
  - 【CVE-2026-3909】Google Skia Out-of-Bounds Write Vulnerability (CVSS v3.1: 8.8)
  - 【是否遭勒索軟體利用:未知】 Google Skia 存在越界寫入漏洞，可能允許遠端攻擊者透過特製的 HTML 頁面執行越界記憶體存取。
  - 此漏洞影響 Google Chrome【ChromeOS【Android【Flutter】以及其他可能使用 Skia 的產品。
- 影響平台:
  - 【CVE-2021-22054】請參考官方所列的影響版本 https://kb.omnissa.com/s/article/87167
  - 【CVE-2025-26399】請參考官方所列的影響版本 https://www.solarwinds.com/trust-center/security-advisories/cve-2025-26399
  - 【CVE-2026-1603】請參考官方所列的影響版本 https://hub.ivanti.com/s/article/Security-Advisory-EPM-February-2026-for-EPM-2024
  - 【CVE-2025-68613】請參考官方所列的影響版本 https://github.com/n8n-io/n8n/security/advisories/GHSA-v98v-ff95-f3cp
  - 【CVE-2026-3910】請參考官方所列的影響版本 https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.ht

ml
    - CVE-2026-3909請參考官方所列的影響版本 https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html
- 建議措施:
    - CVE-2021-22054 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://kb.omnissa.com/s/article/87167
    - CVE-2025-26399 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://www.solarwinds.com/trust-center/security-advisories/cve-2025-26399
    - CVE-2026-1603 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/Security-Advisory-EPM-February-2026-for-EPM-2024
    - CVE-2025-68613 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://github.com/n8n-io/n8n/security/advisories/GHSA-v98v-ff95-f3cp
    - CVE-2026-3910 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html
    - CVE-2026-3909 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html

---

計算機與通訊中心
網路系統組 敬啟