張貼日期：2025/07/10

【漏洞預警】CISA新增4個已知遭駭客利用之漏洞至KEV目錄(2025/06/30-2025/07/06)

- 主旨說明:【漏洞預警】CISA新增4個已知遭駭客利用之漏洞至KEV目錄(2025/06/30-2025/07/06)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202507-00000004
  1. 【CVE-2025-6543】Citrix NetScaler ADC and Gateway Buffer Overflow Vulnerability (CVSS v3.1: 9.8)
     - 【是否遭勒索軟體利用:未知】 Citrix NetScaler ADC和Gateway存在緩衝區溢位漏洞，可能導致非預期的控制流程改變及阻斷服務。
     - 【影響平台】請參考官方所列的影響版本
     - https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788
  2. 【CVE-2025-48928】TeleMessage TM SGNL Exposure of Core Dump File to an Unauthorized Control Sphere Vulnerability (CVSS v3.1: 4.0)
     - 【是否遭勒索軟體利用:未知】 TeleMessage TM SGNL存在核心轉儲檔案暴露於未經授權控制範圍的漏洞。可能透過包含身分驗證資料的記憶體轉儲檔案洩漏敏感資訊。
     - 【影響平台】 TeleMessage 2025-05-05(含)之前的版本
  3. 【CVE-2025-48927】TeleMessage TM SGNL Initialization of a Resource with an Insecure Default Vulnerability (CVSS v3.1: 5.3)
     - 【是否遭勒索軟體利用:未知】 TeleMessage TM SGNL存在以不安全預設值初始化資源的漏洞。此漏洞與Spring Boot Actuator的設定方式有關，當堆轉儲端點暴露於/heapdump URI時，可能導致安全風險。
     - 【影響平台】 TeleMessage 2025-05-05(含)之前的版本
  4. 【CVE-2025-6554】Google Chromium V8 Type Confusion Vulnerability (CVSS v3.1: 8.1)
     - 【是否遭勒索軟體利用:未知】 Google Chromium V8存在類型混淆漏洞，遠端攻擊者可透過特製的HTML網頁執行任意讀寫。此漏洞可能影響多種使用Chromium的網頁瀏覽器，包括但不限於Google Chrome、Microsoft Edge及Opera。
     - 【影響平台】請參考官方所列的影響版本
     - https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_30.html
- 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-2025-6543】 官方已針對漏洞釋出修復更新，請更新至相關版本
     - https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788
  2. 【CVE-2025-48928】 受影響的產品暫無有效緩解措施。建議使用者停止使用相關產品。
  3. 【CVE-2025-48927】 受影響的產品暫無有效緩解措施。建議使用者停止使用相關產品。
  4. 【CVE-2025-6554】 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/2025/06/stable-channel-update-for-desktop_30.html

計算機與通訊中心
網路系統組 敬啟