張貼日期：2025/08/04

【漏洞預警】CISA新增6個已知遭駭客利用之漏洞至KEV目錄(2025/07/21-2025/07/27)

- 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(2025/07/21-2025/07/27)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202507-00000023

1. 【CVE-2025-2775】SysAid On-Prem Improper Restriction of XML External Entity Reference Vulnerability (CVSS v3.1: 9.3)
   - 【是否遭勒索軟體利用:未知】 SysAid On-Prem在Checkin處理功能中存在對XML外部實體參考的不當限制漏洞，可能允許攻擊者接管管理員帳號並讀取任意檔案。
   - 【影響平台】請參考官方所列的影響版本
   - https://documentation.sysaid.com/docs/24-40-60
2. 【CVE-2025-2776】SysAid On-Prem Improper Restriction of XML External Entity Reference Vulnerability (CVSS v3.1: 9.8)
   - 【是否遭勒索軟體利用:未知】 SysAid On-Prem在伺服器URL處理功能中存在對XML外部實體參考的不當限制漏洞，可能允許攻擊者接管管理員帳號並讀取任意檔案。
   - 【影響平台】請參考官方所列的影響版本
   - https://documentation.sysaid.com/docs/24-40-60
3. 【CVE-2025-6558】Google Chromium ANGLE and GPU Improper Input Validation Vulnerability (CVSS v3.1: 8.8)
   - 【是否遭勒索軟體利用:未知】 Google Chromium在ANGLE與GPU元件中存在輸入驗證不當漏洞，攻擊者可透過特製的HTML頁面實現沙箱逃逸。此漏洞可能影響多款基於Chromium的網頁瀏覽器，包括但不限於Google Chrome、Microsoft Edge和Opera。
   - 【影響平台】請參考官方所列的影響版本
   - https://chromereleases.googleblog.com/2025/07/stable-channel-update-for-desktop_15.html
4. 【CVE-2025-54309】CrushFTP Unprotected Alternate Channel Vulnerability (CVSS v3.1: 9.0)
   - 【是否遭勒索軟體利用:未知】 CrushFTP存在未受保護的替代通道漏洞。當未啟用DMZ Proxy功能時，系統錯誤處理AS2驗證，可能允許遠端攻擊者透過HTTPS取得管理員存取權限。
   - 【影響平台】請參考官方所列的影響版本
   - https://www.crushftp.com/crush11wiki/Wiki.jsp?page=CompromiseJuly2025
5. 【CVE-2025-49704】Microsoft SharePoint Code Injection Vulnerability (CVSS v3.1: 8.8)
   - 【是否遭勒索軟體利用:是】 Microsoft SharePoint存在程式碼注入漏洞，可能允許已授權的攻擊者透過網路執行任意程式碼。
   - 【影響平台】請參考官方所列的影響版本
   - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49704
6. 【CVE-2025-49706】Microsoft SharePoint Improper Authentication Vulnerability (CVSS v3.1: 6.5)
   - 【是否遭勒索軟體利用:是】 Microsoft SharePoint存在驗證不當漏洞，可能允許已授權的攻擊者透過網路進行身分偽造。若成功被利用，攻擊者可檢視敏感資訊，並對部分已揭露資訊進行修改。
   - 【影響平台】請參考官方所列的影響版本
   - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49706

- 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-2025-2775 官方已針對漏洞釋出修復更新，請更新至相關版本
        - https://documentation.sysaid.com/docs/24-40-60
    2. CVE-2025-2776 官方已針對漏洞釋出修復更新，請更新至相關版本
        - https://documentation.sysaid.com/docs/24-40-60
    3. CVE-2025-6558 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/2025/07/stable-channel-update-for-desktop_15.html
    4. CVE-2025-54309 官方已針對漏洞釋出修復更新，請更新至相關版本
        - https://www.crushftp.com/crush11wiki/Wiki.jsp?page=CompromiseJuly2025
    5. CVE-2025-49704 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-2025-49704
    6. CVE-2025-49706 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-2025-49706

計算機與通訊中心
網路系統組 敬啟