張貼日期：2025/04/01

【漏洞預警】CISA新增4個已知遭駭客利用之漏洞至KEV目錄(2025/03/24-2025/03/30)

- 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(2025/03/24-2025/03/30)
- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202504-00000001
  - 【CVE-2025-30154】reviewdog/action-setup GitHub Action Embedded Malicious Code Vulnerability (CVSS v3.1: 8.6)
    - 【是否遭勒索軟體利用:未知】 reviewdog action-setup GitHub Action存在嵌入式惡意程式碼漏洞，將洩漏的資訊轉存到Github Actions工作流程日誌。
    - 【影響平台】請參考官方所列的影響版本 https://github.com/reviewdog/reviewdog/security/advisories/GHSA-qmg3-hpqr-gqvc
  - 【CVE-2019-9875】Sitecore CMS and Experience Platform (XP) Deserialization Vulnerability (CVSS v3.1: 8.8)
    - 【是否遭勒索軟體利用:未知】 Sitecore CMS和Experience Platform(XP)在Sitecore.Security.AntiCSRF模組中存在反序列化漏洞，允許經身分驗證的攻擊者透過在HTTP POST參數__CSRFTOKEN中傳送序列化的.NET物件執行任意程式碼。
    - 【影響平台】請參考官方所列的影響版本 https://support.sitecore.com/kb?id=kb_search
  - 【CVE-2019-9874】Sitecore CMS and Experience Platform (XP) Deserialization Vulnerability (CVSS v3.1: 9.8)
    - 【是否遭勒索軟體利用:未知】 Sitecore CMS和Experience Platform(XP)在Sitecore.Security.AntiCSRF模組中存在反序列化漏洞，允許未經身分驗證的攻擊者透過在HTTP POST參數__CSRFTOKEN中傳送序列化的.NET物件執行任意程式碼。
    - 【影響平台】請參考官方所列的影響版本 https://kb.sitecore.net/articles/334035
  - 【CVE-2025-2783】Google Chromium Mojo Sandbox Escape Vulnerability (CVSS v3.1: 8.3)
    - 【是否遭勒索軟體利用:未知】 Windows上的Google Chromium Mojo存在因邏輯錯誤導致的沙箱逃逸漏洞，該漏洞源於在未指定情況下提供不正確的句柄，可能影響包括Google Chrome、Microsoft Edge和Opera在內的多個Chromium瀏覽器。
    - 【影響平台】請參考官方所列的影響版本 https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_25.html
- 影響平台: 詳細內容於內容說明欄之影響平台
- 建議措施:
  - 【CVE-2025-30154】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://github.com/reviewdog/reviewdog/security/advisories/GHSA-qmg3-hpqr-gqvc
  - 【CVE-2019-9875】 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?id=kb_search
  - 【CVE-2019-9874】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://kb.sitecore.net/articles/334035
  - 【CVE-2025-2783】 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/2025/03/stable-channel-update-for-desktop_25.html

---

計算機與通訊中心

網路系統組 敬啟