張貼日期：2026/04/28

【漏洞預警】CISA新增3個已知遭駭客利用之漏洞至KEV目錄(2026/03/30-2026/04/05)

- 主旨說明:【漏洞預警】CISA新增3個已知遭駭客利用之漏洞至KEV目錄(2026/03/30-2026/04/05)

- 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-200-202604-00000005
  - 【CVE-2026-3055】Citrix NetScaler Out-of-Bounds Read Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 Citrix NetScaler ADC【NetScaler Gateway 以及 NetScaler ADC FIPS 和 NDcPP 在被配置為 SAML IDP時，存在越界讀取漏洞，可能導致記憶體過度讀取。
  - 【CVE-2026-5281】Google Dawn Use-After-Free Vulnerability (CVSS v3.1: 8.8)
  - 【是否遭勒索軟體利用:未知】 Google Dawn 存在使用釋放後記憶體漏洞，可能允許已入侵渲染程序的遠端攻擊者，透過特製的 HTML 頁面執行任意程式碼。此漏洞可能影響多個基於 Chromium 的產品，包括但不限於 Google Chrome【Microsoft Edge 及 Opera】
  - 【CVE-2026-3502】TrueConf Client Download of Code Without Integrity Check Vulnerability (CVSS v3.1: 7.8)
  - 【是否遭勒索軟體利用:未知】 TrueConf Client 存在下載程式碼時未進行完整性檢查的漏洞。攻擊者若能影響更新傳輸路徑，可能替換為經竄改的更新酬載；一旦被更新程式執行或安裝，可能導致在更新程序或使用者權限範圍內執行任意程式碼。
- 影響平台:
  - 【CVE-2026-3055】請參考官方所列的影響版本 https://support.citrix.com/support-home/home
  - 【CVE-2026-5281】請參考官方所列的影響版本 https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html
  - 【CVE-2026-3502】TrueConf 8.1.0至8.5.2(含)的版本
- 建議措施:
  - 【CVE-2026-3055】 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/home
  - 【CVE-2026-5281】 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_31.html
  - 【CVE-2026-3502】 對應產品升級至以下版本(或更高) TrueConf 8.5.3.884

計算機與通訊中心
網路系統組 敬啟