張貼日期：2025/11/18

【漏洞預警】CISA新增5個已知遭駭客利用之漏洞至KEV目錄(2025/11/10-2025/11/16)

- 主旨說明:【漏洞預警】CISA新增5個已知遭駭客利用之漏洞至KEV目錄(2025/11/10-2025/11/16)

- 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-200-202511-00000012
  - 【CVE-2025-21042】Samsung Mobile Devices Out-of-Bounds Write Vulnerability (CVSS v3.1: 8.8)
  - 【是否遭勒索軟體利用:未知】 三星行動裝置在 libimagecodec.quram.so 中存在越界寫入漏洞。該漏洞可能使遠端攻擊者得以執行任意程式碼。
  - 【CVE-2025-12480】Gladinet Triofox Improper Access Control Vulnerability (CVSS v3.1: 9.1)
  - 【是否遭勒索軟體利用:未知】 Gladinet Triofox 存在不當存取控制漏洞，該漏洞允許在設定完成後仍可存取初始設定頁面。
  - 【CVE-2025-62215】Microsoft Windows Race Condition Vulnerability (CVSS v3.1: 7.0)
  - 【是否遭勒索軟體利用:未知】 Microsoft Windows 核心存在競爭條件漏洞，允許具低階權限的本機攻擊者提升權限。成功利用此漏洞後，攻擊者可能取得 SYSTEM 級別存取權限。
  - 【CVE-2025-9242】WatchGuard Firebox Out-of-Bounds Write Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 WatchGuard Firebox 的作業系統中 iked 程序存在越界寫入漏洞，可能允許未經認證的遠端攻擊者執行任意程式碼。
  - 【CVE-2025-64446】Fortinet FortiWeb Path Traversal Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 Fortinet FortiWeb 存在相對路徑遍歷漏洞，未經驗證的攻擊者可透過特製的 HTTP 或 HTTPS 請求在系統上執行管理指令。
- 影響平台:
  - 【CVE-2025-21042】請參考官方所列的影響版本 https://security.samsungmobile.com/securityUpdate.smsb
  - 【CVE-2025-12480】TrioFox 16.7.10368.56560(含)之前的版本
  - 【CVE-2025-62215】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62215
  - 【CVE-2025-9242】請參考官方所列的影響版本 https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00015
  - 【CVE-2025-64446】請參考官方所列的影響版本 https://fortiguard.fortinet.com/psirt/FG-IR-25-910
- 建議措施:
  - 【CVE-2025-21042】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://security.samsungmobile.com/securityUpdate.smsb
  - 【CVE-2025-12480】 對應產品升級至以下版本(或更高) TrioFox 16.7.10368.56560(不含)之後的版本
  - 【CVE-2025-62215】 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-2025-62215
  - 【CVE-2025-9242】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00015
  - 【CVE-2025-64446】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://fortiguard.fortinet.com/psirt/FG-IR-25-910

計算機與通訊中心
網路系統組 敬啟