張貼日期：2025/05/14

【漏洞預警】CISA新增4個已知遭駭客利用之漏洞至KEV目錄(2025/05/05-2025/05/11)

- 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(2025/05/05-2025/05/11)
- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202505-00000008
  1. 【CVE-2025-3248】Langflow Missing Authentication Vulnerability (CVSS v3.1: 9.8)
     【是否遭勒索軟體利用:未知】 Langflow在/api/v1/validate/code端點中存在驗證缺失漏洞，允許遠端未經驗證的攻擊者透過特製的 HTTP請求執行任意程式碼。
     【影響平台】 langflow 1.2.0(含)之前的版本
  2. 【CVE-2025-27363】FreeType Out-of-Bounds Write Vulnerability (CVSS v3.1: 8.1)
     【是否遭勒索軟體利用:未知】 FreeType在嘗試解析與TrueType GX和可變字型檔案相關的子字型結構時，存在越界寫入漏洞，可能導致任意程式碼執行。
     【影響平台】 FreeType 2.13.0(含)之前的版本
  3. 【CVE-2024-11120】GeoVision Devices OS Command Injection Vulnerability (CVSS v3.1: 9.8)
     【是否遭勒索軟體利用:未知】 多款 GeoVision 裝置存在作業系統指令注入漏洞，遠端未經驗證的攻擊者可藉此注入並執行任意系統指令。
     【影響平台】 GV-VS12 GV-VS11 GV-DSP_LPR_V3 GVLX 4 V2 GVLX 4 V3
  4. 【CVE-2024-6047】GeoVision Devices OS Command Injection Vulnerability (CVSS v3.1: 9.8)
     【是否遭勒索軟體利用:未知】 多款 GeoVision 裝置存在作業系統指令注入漏洞，遠端未經驗證的攻擊者可藉此注入並執行任意系統指令。
     【影響平台】 GV_DSP_LPR_V2 GV_IPCAMD_GV_BX130 GV_IPCAMD_GV_BX1500 GV_IPCAMD_GV_CB220 GV_IPCAMD_GV_EBL1100 GV_IPCAMD_GV_EFD1100 GV_IPCAMD_GV_FD2410 GV_IPCAMD_GV_FD3400 GV_IPCAMD_GV_FE3401 GV_IPCAMD_GV_FE420 GV_GM8186_VS14 GV-VS14_VS14 GV_VS03 GV_VS2410 GV_VS28XX GV_VS216XX GV VS04A GV VS04H GVLX 4 V2 GVLX 4 V3
- 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-2025-3248】 對應產品升級至以下版本(或更高) langflow 1.3.0
  2. 【CVE-2025-27363】 對應產品升級至以下版本(或更高) FreeType 2.13.1
  3. 【CVE-2024-11120】 受影響的產品可能已達到生命週期終止(EoL)或服務終止(EoS)，建議使用者停止使用相關產品。
  4. 【CVE-2024-6047】 受影響的產品可能已達到生命週期終止(EoL)或服務終止(EoS)，建議使用者停止使用相關產品。

計算機與通訊中心
網路系統組 敬啟

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20250514_04

Last update: **2025/05/14 15:50**