張貼日期：2025/01/02

【漏洞預警】全景軟體CGFIDO 存在二個高風險資安漏洞

- 主旨說明:全景軟體CGFIDO 存在二個高風險資安漏洞
- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202412-00000003
  - 【全景軟體CGFIDO - Authentication Bypass(TVN-202412008,CVE-2024-12838,CVSS:8.8) 全景軟體CGFIDO之無密碼登入機制存在Authentication Bypass漏洞，已取得一般權限之遠端攻擊者可發送特製請求變更為任意使用者，包含管理員。
    - 影響產品:CGFIDO 0.0.1 至 1.1.0版本
    - 建議措施：更新至1.2.0(含)以後版本
  - 【全景軟體CGFIDO - Authentication Bypass(TVN-202412009,CVE-2024-12839,CVSS:8.8) 全景軟體CGFIDO之設備驗證登入機制存在Authentication Bypass by Capture-replay漏洞，若使用者存取偽造網站，其設備部署的agent程式便會發送驗證簽章至該網站，未經身分鑑別之遠端攻擊者在取得此簽章後便可使用任意設備登入系統。
    - 影響產品:CGFIDO 1.2.1(含)以前版本
    - 建議措施：更新至1.2.2(含)以後版本
- 影響平台:
  - CGFIDO 0.0.1 至 1.1.0版本
  - CGFIDO 1.2.1(含)以前版本
- 建議措施:根據情資內容，更新至對應版本
- 參考資料:
  1. 全景軟體CGFIDO - Authentication Bypass:https://www.twcert.org.tw/tw/cp-132-8332-2100f-1.html
  2. 全景軟體 CGFIDO - Authentication Bypass:https://www.twcert.org.tw/tw/cp-132-8334-8b836-1.html

---

計算機與通訊中心
網路系統組 敬啟