張貼日期：2023/12/21

【漏洞預警】凱發科技 WebITR 差勤系統存在漏洞，建議請管理者儘速評估更新！

- 主旨說明：凱發科技 WebITR 差勤系統存在漏洞，建議請管理者儘速評估更新！
- 內容說明：
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202312-00000001
  - 凱發科技 WebITR 差勤系統漏洞說明如下:
    - CVE-2023-48395 凱發科技 WebITR 差勤系統存在SQL Injection漏洞，一般權限的遠端攻擊者，可以注入任意 SQL 查詢指令以讀取資料庫內容。
    - CVE-2023-48394 凱發科技 WebITR 差勤系統之上傳功能未對上傳檔案進行檢查限制，並可上傳檔案至任意位置。具一般使用者權限之遠端攻擊者導登入系統後，即可以上傳任意檔案，進而執行任意程式碼或中斷系統服務。
    - CVE-2023-48393 凱發科技 WebITR 差勤系統存在Error Message Leakage漏洞，具一般權限的遠端攻擊者，可從網頁服務回傳的錯誤訊息中取得部分系統資訊。
    - CVE-2023-48392 凱發科技 WebITR 差勤系統使用固定的加密金鑰，不具權限遠端攻擊者可以自行產生合法的 token 參數，並能以任意使用者身分登入該系統，取得系統內資料與執行相關流程。
- 影響平台:
  - 凱發科技 WebITR 差勤系統2_1_0_23
- 建議措施:
  - 更新至最新版本
- 參考資料:
  - https://www.twcert.org.tw/tw/lp-132-1.html

計算機與通訊中心
網路系統組 敬啟