

張貼日期: 2024/04/01

【漏洞預警】凱發科技WebITR差勤系統存在多個高風險安全漏洞(CVE-2023-48392至CVE-2023-48395)請儘速確認並進行修補!

- 主旨說明: 凱發科技WebITR差勤系統存在多個高風險安全漏洞(CVE-2023-48392至CVE-2023-48395)請儘速確認並進行修補!
- 內容說明:
 - 轉發 國家資安資訊分享與分析中心 NISAC-200-202403-00000178
 - 研究人員發現, 凱發科技WebITR差勤系統存在多個高風險安全漏洞(CVE-2023-48392至CVE-2023-48395)其中CVE-2023-48392與CVE-2023-48394之漏洞評分高達8.8分以上, 且漏洞目前已遭駭客利用, 請儘速確認並進行修補。
 - CVE-2023-48392 WebITR差勤系統使用固定加密金鑰, 遠端攻擊者可以自行產生合法Token參數, 即可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。
 - CVE-2023-48394 WebITR差勤系統之上傳功能未對上傳檔案進行檢查, 並可上傳檔案至任意位置。遠端攻擊者透過一般使用者權限帳號登入系統後, 即可上傳任意檔案, 進而執行任意程式碼或中斷系統服務。
- 影響平台:
 - WebITR差勤系統2_1_0_19(含)以下版本
- 建議措施:
 - 官方已針對漏洞釋出修復更新, 請更新至以下版本 WebITR差勤系統2_1_0_23(含)以上版本

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:20240401_03

Last update: 2024/04/01 16:20