張貼日期：2017/09/27

[資安漏洞預警通知]特定考勤門禁系統存在資安漏洞，恐遭利用進行虛擬貨幣挖礦或對外攻擊

主旨：特定考勤門禁系統存在資安漏洞，恐遭利用進行虛擬貨幣挖礦或對外攻擊

說明：

1. 技服中心發現特定考勤門禁系統存在以下漏洞：
    1. 使用公開的網際網路位址，且對外開啟多個服務如SSH、Telnet及Web。
    2. 未變更系統預設帳號密碼，使外部人員得以取得管理者身分進行系統操作。
    3. 外部人員可針對相關服務漏洞進行探測攻擊亦或使用工具進行暴力破解行為。
    4. 設備系統Web服務未做網址路徑限制存取設定，使外部使用者無須身分驗證，即可透過連線特定網址路徑進行系統操作，如：開啟門禁、修改設備網際網路位址、新增、列舉及刪除使用者帳號資訊。
    5. 設備系統存在SQL Injection漏洞，造成系統敏感資訊洩漏，如使用者帳密、內部人員出勤紀錄及系統設定參數等。
2. 上述系統漏洞可能會造成相關資安風險如下：
    1. 設備系統連線至外部虛擬貨幣挖礦主機，進行虛擬貨幣挖礦行為。
    2. 設備系統遭植入惡意程式，並對外進行漏洞探測與攻擊行為。
    3. 設備系統遭入侵成為殭屍網路成員，並對外進行阻斷式服務攻擊行為。
3. 影響平臺： 具聯網功能之臉型或指紋辨識之門禁考勤系統
4. 建議措施：
    1. 盤點與檢視是否使用相關考勤門禁系統
    2. 相關設備系統應置於防火牆後端並設置防火牆規則，將內網與外網做分隔以防外部非法人士登入。
    3. 關閉系統上不必要的網路服務，以防遭漏洞探測。
    4. 系統上所有帳號需設定強健的密碼並定期更換，非必要使用的帳號請將其刪除或停用。
    5. 若確認該設備已遭入侵，建議聯繫相關設備廠商重新安裝系統，並注意須安裝至最新修補程式。若暫時未發現異常行為，建議持續觀察一個星期左右。
    6. 建議透過防火牆紀錄持續觀察與監控相關設備是否有異常活動行為，例如：外部探測攻擊、密碼暴力破解及阻斷式服務攻擊等。

計算機與通訊中心
網路系統組 敬啟