張貼日期：2022/09/12

【攻擊活動訊息QNAP 提醒用戶近期出現針對 NAS 暴露外網並有安裝 Photo Station 裝置，發動DeadBolt勒贖攻擊

- 主旨說明QNAP 提醒用戶近期出現針對 NAS 暴露外網並有安裝 Photo Station 裝置，發動DeadBolt勒贖攻擊。

- 內容說明：
  - 轉發 台灣電腦網路危機處理暨協調中心(TWCERT/CC)
  - 在 QNAP 發表的資安通報中指出DeadBolt勒贖攻擊主要針對【暴露外網並有安裝 Photo Station裝置】，如果裝置使用預設登入帳號與弱密碼，就很可能遭到駭侵者成功登入，並將裝置上的檔案進行加密。
- 影響平台: \\運行 Photo Station 並在互聯網上曝光的 QNAP NAS裝置。
- 建議措施:
  1. 關閉路由器的端口轉發(port forwarding)功能。
  2. 在 NAS 上設置 myQNAPcloud 以啟用安全遠程訪問並防止暴露在互聯網上。
  3. 在系統防火牆中設定規則，將多次嘗試登入失敗的 IP 列入黑名單，禁止再次連線。
  4. 將使用中的 QNAP 裝置上之應用程序、韌體更新到最新版本。
  5. 立即審視所有 NAS 上的使用者帳號，確認密碼強度足夠。
  6. 將系統預設的 admin 帳號停用，改用其他不容易被猜到的帳號設定為系統管理員專用帳號。
  7. 定期備份檔案並執行檔案快照作業。
- 參考資料: https://www.qnap.com/zh-tw/security-advisory/qsa-22-24

計算機與通訊中心
網路系統組 敬啟