張貼日期：2022/05/23

【資安漏洞預警】威聯通科技(QNAP)偵測到有不法分子濫用日前已修補的安全性問題 (qsa-21-57) 發動網路攻擊

- 主旨說明：威聯通科技(QNAP)偵測到有不法分子濫用日前已修補的安全性問題 (qsa-21-57) 發動網路攻擊

- 內容說明：
  - 轉發 台灣電腦網路危機處理暨協調中心(TWCERT/CC)
  - 威聯通 ® 科技 (QNAP® Systems, Inc.) 近日偵測到 DEADBOLT Ransomware 發動新的攻擊。依據 QNAP 產品資安事件應變團隊 (QNAP PSIRT) 的調查顯示：此次攻擊鎖定使用 QTS 4.3.6 與 QTS 4.4.1 的 NAS 設備，受影響機型以 TS-x51 系列及 TS-x53 系列為主QNAP 呼籲所有 NAS 用戶儘速檢查並更新 QTS 至最新版本，並避免將 NAS 暴露於外網。
- 影響平台：
  - 受影響之QNAP設備如下：
    - QNAP機型 TS-x51 系列及 TS-x53 系列為主
  - 受影響之QNAP軟體如下：
    - 使用QTS 4.3.6 與 QTS 4.4.1 的 NAS 設備。
- 建議措施：建議不管何種機型，因儘速檢查並更新QTS至最新版本，並避免將 NAS 暴露於外網。
- 參考資料：
  1. 立即採取資安防護行動，更新 QTS 至最新版本 | QNAP https://www.qnap.com/zh-tw/security-news/2022/%E7%AB%8B%E5%8D%B3%E6%8E%A1%E5%8F%96%E8%B3%87%E5%AE%89%E9%98%B2%E8%AD%B7%E8%A1%8C%E5%8B%95%E6%9B%B4%E6%96%B0-qts-%E8%87%B3%E6%9C%80%E6%96%B0%E7%89%88%E6%9C%AC
  2. https://www.qnap.com/zh-tw/security-advisory/qsa-21-57
  3. 立即速更新 QTS 至最新版本及避免將 NAS 暴露於外網，共同打擊網路犯罪 https://www.qnap.com/zh-tw/security-news/2022/%E7%AB%8B%E5%8D%B3%E9%80%9F%E6%9B%B4%E6%96%B0-qts-%E8%87%B3%E6%9C%80%E6%96%B0%E7%89%88%E6%9C%AC%E5%8F%8A%E9%81%BF%E5%85%8D%E5%B0%87-nas-%E6%9A%B4%E9%9C%B2%E6%96%BC%E5%A4%96%E7%B6%B2%E5%85%B1%E5%90%8C%E6%89%93%E6%93%8A%E7%B6%B2%E8%B7%AF%E7%8A%AF%E7%BD%AA
  4. 有關「建議版本」功能之說明 | QNAP https://www.qnap.com/zh-tw/security-news/2022/%E6%9C%89%E9%97%9C%E5%BB%BA%E8%AD%B0%E7%89%88%E6%9C%AC%E5%8A%9F%E8%83%BD%E4%B9%8B%E8%AA%AA%E6%98%8E

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:20220523_01

Last update: **2022/05/23 09:48**