張貼日期：2020/05/25

【資安漏洞預警□QNAP NAS設備存在安全漏洞(CVE-2019-7192□CVE-2019-7193□CVE-2019-7194及CVE-2019-7195)□允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新

主旨：【資安漏洞預警□QNAP NAS設備存在安全漏洞(CVE-2019-7192□CVE-2019-7193□CVE-2019-7194及CVE-2019-7195)□允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202005-0537□
  - 研究人員發現QNAP NAS設備使用之Photo Station應用程式，存在任意檔案讀取與程式碼注入等安全漏洞(CVE-2019-7192□CVE-2019-7193□CVE-2019-7194及CVE-2019-7195)□遠端攻擊者可對目標設備發送特製請求，利用此漏洞進而執行任意程式碼。
- 影響平台:
  啟用Photo Station應用程式之QNAP設備皆受此漏洞影響
- 建議措施:
  - 目前QNAP官方已針對此漏洞釋出更新程式，請各機關聯絡設備維護廠商進行版本確認並將設備更新至以下版本：
    - QTS□
      QTS 4.4.1□build 20190918(含)以後版本
      QTS 4.3.6□build 20190919(含)以後版本
    - Photo Station□
      QTS 4.4.1□Photo Station 6.0.3(含)以後版本
      QTS 4.3.4 ~ QTS 4.4.0□Photo Station 5.7.10(含)以後版本
      QTS 4.3.0 ~ QTS 4.3.3□Photo Station 5.4.9(含)以後版本
      QTS 4.2.6□Photo Station 5.2.11(含)以後版本
  - 官方公告連結如下：https://www.qnap.com/zh-tw/security-advisory/nas-201911-25
- 參考資料:
  1. https://www.qnap.com/zh-tw/security-advisory/nas-201911-25
  2. https://www.ithome.com.tw/news/137748

計算機與通訊中心
網路系統組 敬啟