

張貼日期：2024/04/01

【漏洞預警】QNAP OS存在高風險安全漏洞(CVE-2024-21899)請儘速確認並進行修補！

- 主旨說明：QNAP OS存在高風險安全漏洞(CVE-2024-21899)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-200-202403-00000208
 - 研究人員發現QNAP OS存在不當驗證(Improper Authentication)漏洞(CVE-2024-21899)遠端攻擊者可利用此漏洞繞過身分鑑別，取得系統控制，請儘速確認並進行修補。
- 影響平台：
 - QTS 4.5.x[5.1.x
 - QuTS hero h4.5.x[h5.1.x
 - QuTScLOUD c5.x
 - myQNAPcloud 1.0.x
- 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：
 - QTS 4.5.4.2627 build 20231225(含)以上版本
 - QTS 5.1.3.2578 build 20231110(含)以上版本
 - QuTS hero h4.5.4.2626 build 20231225(含)以上版本
 - QuTS hero h5.1.3.2578 build 20231110(含)以上版本
 - QuTScLOUD c5.1.5.2651(含)以上版本
 - myQNAPcloud 1.0.52 (2023/11/24)(含)以上版本 * 參考資料：
- 參考資料：
 - <https://nvd.nist.gov/vuln/detail/CVE-2024-21899>

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/mailling:announcement:20240401_01



Last update: **2024/04/01 16:01**