張貼日期：2022/02/23

【資安攻擊預警】為防範 ASUSTOR NAS 遭 DeadBolt 勒索病毒攻擊，建議相關用戶立即進行資安防護！

- 主旨說明：為防範 ASUSTOR NAS 遭 DeadBolt 勒索病毒攻擊，建議相關用戶立即進行資安防護！

- 內容說明：
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-ANA-202202-0001
  - 因應 DeadBolt 勒索病毒攻擊ASUSTOR Inc. 目前暫時停止 EZ-Connect ASUSTOR EZ Connectezconnect.to 服務，並研究勒索病毒的根源與解決方案。為了保護您的資料，避免 DeadBolt 勒索病毒的攻擊綁架，建議採取下列措施。
- 影響平台:
  - ASUSTOR NAS
- 建議措施:
  1. 更改預設 ADM 8000 及 8001 等連接埠與 Web 服務 80 及 443 等連接埠。
  2. 關閉 EZ-Connect 服務
  3. 立即備份
  4. 若不須使用 SSH SFTP 服務，請將其停用。
     更詳細安全措施，如附參考資料。
     - 如果已發現自己的 NAS 已遭遇 DeadBolt 勒索病毒的綁架攻擊，請先拔除網路線與關機(按3秒電源開關，聽到嗶聲)，並於ASUSTOR官方表單(https://docs.google.com/forms/d/e/1FAIpQLSfZ7gjxKSHiqMZoQHl7-Dm7OfbgpKJIyylq7Hg4bY5RwUJK9g/viewform) 留下您的資訊ASUSTOR 的技術人員將盡快與您聯繫。
     - TWCERT發布相關資安新聞，連結：https://www.twcert.org.tw/tw/cp-104-5756-e9900-1.html
- 參考資料:
  1. https://www.asustor.com/zh-tw/online/College_topic?topic=353#2
  2. https://docs.google.com/forms/d/e/1FAIpQLSfZ7gjxKSHiqMZoQHl7-Dm7OfbgpKJIyylq7Hg4bY5RwUJK9g/viewform
  3. https://www.asustor.com/zh-tw/knowledge/detail/?id=6&group_id=628

計算機與通訊中心
網路系統組 敬啟