張貼日期：2021/06/24

【資安訊息】近期勒索軟體攻擊活動頻繁，請加強系統/應用程式更新與防範作業 ！

主旨：【資安訊息】近期勒索軟體攻擊活動頻繁，請加強系統/應用程式更新與防範作業 ！

- 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 NCCST-ANA-2021-0000241
  - 近期勒索軟體攻擊頻繁，攻擊範圍涉及交通、能源、醫療與金融領域，技服中心亦接獲多個政府機關通報遭感染勒索軟體事件，目前已知駭客利用漏洞如下：
    - Fortinet VPN 設備漏洞 (CVE-2018-13379)
    - Ivanti VPN 設備Pulse Connect Secure 漏洞 (CVE-2021-22893、CVE-2020-8260、CVE-2020-8243、CVE-2019-11510)
    - Citrix Application Delivery Controller、Citrix Gateway、Citrix SD-WAN WANOP 漏洞 (CVE-2019-19781)
    - Microsoft Exchange Server 漏洞 (CVE-2021-26855 等)
    - SonicWall SMA100 漏洞 (CVE-2021-20016)
    - QNAP NAS 漏洞 (CVE-2021-28799、CVE-2020-36195、CVE-2020-2509 等)
    - Windows Domain Controller 漏洞 (CVE-2020-1472等)
    - Internet Explorer 漏洞 (CVE-2018-8174等)
  - 建議請各級政府機關除加強組織資安監控防護外，持續確認相關應用程式更新情況，定期備份重要檔案，加強資訊安全宣導，避免開啟來路不明郵件或連結。
- 影響平台：全
- 建議措施：
  1. 清查機關是否有使用被已知勒索軟體利用之軟體與設備，並及時完成漏洞修補。
  2. 檢視主機對外開放的必要性，無特殊需求建議關閉不必要之通訊埠(如137, 138, 139, 445, 3389等)，僅開放必要服務。
  3. 確認作業系統、防毒軟體，及應用程式(如Adobe Flash Player、Java)更新情況，並定期檢視系統/應用程式更新紀錄，避免駭客利用系統/應用程式安全性漏洞進行入侵行為。
  4. 定期備份系統資料，並參考以下建議措施：
     - 應確保備份資料無感染之虞，例如採用離線備份存放。
     - 定期測試備份資料可有效還原。
     - 針對機敏資料應進行存取控制管控與加密。
  5. 即時監測未授權之存取行為，透過專職監控人員或自動化機制偵測未經授權之存取行為，加強對伺服器、網路設備及個人電腦等設備之日誌監控。
  6. 加強資安教育訓練，使用者留意相關電子郵件，注意郵件之來源的正確性，不要開啟不明來源信件的附檔或連結。
  7. 建立良好的網段管理，確保隔離的網段可以獨自運行。
  8. 利用第三方滲透測試，確認系統安全性與抵禦攻擊的能力。
- 參考資料：
  1. https://www.cnbc.com/2021/06/03/ransomware-attacks-white-house-memo-urges-immediate-action-by-business.html
  2. https://www.ithome.com.tw/news/144869
  3. 日本NISC情資原文： https://www.nisc.go.jp/active/infra/pdf/ransomware20210430.pdf

---

計算機與通訊中心

網路系統組 敬啟