張貼日期：2022/04/08

【資安漏洞預警Trend Micro Apex Central平台存在高風險安全漏洞(CVE-2022-26871)請儘速確認並進行更新！

- 主旨說明Trend Micro Apex Central平台存在高風險安全漏洞(CVE-2022-26871)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 NISAC-ANA-202204-0208
  - 趨勢科技研究中心發現Trend Micro Apex Central平台存在高風險安全漏洞(CVE-2022-26871)肇因於檔案處理方式不當，導致未經授權之攻擊者可上傳任意檔案，進而遠端執行任意程式碼，且已出現利用此漏洞之攻擊行為，請儘速確認並進行更新。
- 影響平台:
  - Trend Micro Apex Central 2019 Build 6016(不含)以前版本。
  - Trend Micro Apex Central as a Service(SaaS) Build 202203(不含)以前版本。
- 建議措施:
  1. Trend Micro官方網頁(https://success.trendmicro.com/dcx/s/solution/000290678?language=en_US)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與更新：
     1. 更新Apex Central 2019至Patch 3(Build 6016)以上版本
     2. Apex Central as a Service(SaaS)已由趨勢科技於2022/3/9完成版本更新，使用者無需執行任何動作
  2. 若無法更新Apex Central 2019至最新版本，請參考Trend Micro官方網頁之Trend Micro Protection一節，透過設定IPS規則進行防護。
  3. 管理者登入Web管理主控台後，可於「說明 – >關於」頁面中得知目前所使用之Apex Central版本。
- 參考資料:
  1. https://www.ithome.com.tw/news/150252
  2. https://success.trendmicro.com/dcx/s/solution/000290678?language=en_US
  3. https://appweb.trendmicro.com/supportNews/NewsDetail.aspx?id=4435
  4. https://success.trendmicro.com/jp/solution/000290660
  5. https://success.trendmicro.com/jp/solution/000265749
  6. https://www.jpcert.or.jp/english/at/2022/at220008.html

計算機與通訊中心
網路系統組 敬啟