張貼日期：2020/03/09

【資安漏洞預警】微軟Exchange伺服器存在安全漏洞(CVE-2020-0688)允許攻擊者遠端執行任意程式碼

主旨：【資安漏洞預警】微軟Exchange伺服器存在安全漏洞(CVE-2020-0688)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-202003-0138
  - CVE-2020-0688肇因於Exchange伺服器未在安裝時建立唯一金鑰，使得攻擊者可透過授權使用者取得金鑰，利用傳遞特製payload到Exchange伺服器，造成記憶體毀損展開攻擊。 攻擊者需先透過授權使用者資訊，以開發者工具取得ViewStateUserKey與__VIEWSTATEGENERATOR值後，利用公開的.NET參數反序列化工具造訪特定頁面，便可遠端執行任意程式碼。
- 影響平台:
  - Microsoft Exchange Server 2010
  - Microsoft Exchange Server 2013
  - Microsoft Exchange Server 2016
  - Microsoft Exchange Server 2019
- 建議措施:
  1. 透過微軟提供版本檢視方式確認Exchange版本資訊(https://docs.microsoft.com/en-us/Exchange/new-features/build-numbers-and-release-dates?redirectedfrom=MSDN&view=exchserver-2019)，並儘速完成Exchange更新作業。
  2. 未能即時完成更新，建議關閉外部存取Exchange Control Panel(ECP)服務，如開放外部存取，則應以白名單方式限制存取來源，確認存取來源皆為授權使用者。
  3. 檢視IIS日誌與Exchange相關紀錄，釐清是否存有異常連線或檔案下載/執行等相關情事，以確認外部利用漏洞入侵疑慮。
  4. 請注意個別系統之安全修補與病毒碼更新，包含作業系統、程式套件及防毒軟體等。
- 參考資料:
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0688
  2. https://www.thezdi.com/blog/2020/2/24/cve-2020-0688-remote-code-execution-on-microsoft-exchange-server-through-fixed-cryptographic-keys
  3. https://www.ithome.com.tw/news/136043

計算機與通訊中心
網路系統組 敬啟