行政院國家資通安全會報技術服務中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2020-0024	發布時間	Thu Mar 05 10:15:20 CST 2020
事件類型	漏洞預警	發現時間	Wed Mar 04 00:00:00 CST 2020
警訊名稱	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	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。 技服中心近期已發現針對微軟 Exchange 伺服器攻擊活動，請機關提高警覺並儘速確認並修補或調整設定，避免機關設備遭入侵。		
影響平台	Microsoft Exchange Server 2010 Microsoft Exchange Server 2013 Microsoft Exchange Server 2016 Microsoft Exchange Server 2019		
影響等級	中		
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

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw