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-2018-0026	發布時間	Fri Mar 16 17:14:25 CST 2018
事件類型	漏洞預警	發現時間	Fri Mar 16 00:00:00 CST 2018
警訊名稱	CredSSP 協定存在安全漏洞(CVE-2018-0866)，導致攻擊者可執行任意程式碼取得使用者權限，並對遠端主機進行操作，請儘速確認並進行修正		
內容說明	CredSSP(Credential Security Support Provider)協定為提供 RDP(Remote Desktop Protocol)與 WinRM(Windows Remote Management)服務所使用認證協定，負責將 Windows 用戶端加密憑證轉發到目標伺服器進行認證。 研究團隊發現 CredSSP 協定存在安全漏洞(CVE-2018-0866)，當使用者向遠端主機進行 RDP 或 WinRM 連線時，攻擊者可在 WiFi 或實體網路環境中，透過中間人攻擊(MITM)去竊取會話(Session)的認證資料，進而造成攻擊者可執行任意程式碼取得使用者權限，並對遠端主機進行操作。		
影響平台	Microsoft Windows 所有版本		
影響等級	高		
建議措施	目前 Microsoft 官方已針對此弱點釋出修補方式，請各機關可聯絡維運廠商或參考以下建議進行修正： 1.請至下列連結依據適當的版本進行更新(https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-0886)或透過微軟的 3 月份自動更新進行修復。 2.更新完成後請參考 Microsoft 官方(https://support.microsoft.com/en-us/help/4093492/credssp-updates-for-cve-2018-0886-march-13-2018)的 Group Policy 設定。 - 請於系統中的 Group Policy 設定，點選「電腦設定」>「系統管理範本」>「系統」>「認證委派」>「Encryption Oracle Remediation」，點選「啟用」並選擇「Mitigated」或「Force Updated Clients」的安全級別。		
參考資料	1.https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-0886		

	2.https://thehackernews.com/2018/03/credssp-rdp-exploit.html 3.https://blog.preempt.com/security-advisory-credssp

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