張貼日期：2018/03/20

[資安漏洞預警通知] Microsoft Windows CredSSP協定存在安全漏洞，請儘速確認並進行修正

主旨：[資安漏洞預警通知] Microsoft Windows CredSSP協定存在安全漏洞，請儘速確認並進行修正

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。
- 影響平臺：
  - Microsoft Windows所有版本
- 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

計算機與通訊中心
網路系統組 敬啟