張貼日期：2017/07/21

［資安漏洞預警通知］微軟Windows作業系統的NTLM驗證通訊協定存在允許攻擊者透過重送攻擊進而取得整個網域控制權之漏洞，請儘速進行更新

主旨：微軟Windows作業系統的NTLM驗證通訊協定存在允許攻擊者透過重送攻擊進而取得整個網域控制權之漏洞，請儘速進行更新

說明：

1. NT LAN Manager (NTLM)驗證通訊協定是微軟的一種安全協定，根據挑戰或回應(Challenge/Response)機制進行使用者身分驗證。研究人員發現NTLM驗證通訊協定存在允許執行輕量型目錄存取通訊協定(LDAP)重送攻擊與遠端桌面協定(RDP)重送攻擊之安全漏洞。
2. LDAP重送攻擊漏洞允許具有本機系統(SYSTEM)權限的攻擊者，利用攔截NTLM登入封包與客製惡意封包傳送到網域控制站，可進行網域操作(如新增網域帳號)，進而取得網域控制權。只要攻擊者先行取得系統(SYSTEM)權限即可利用此漏洞取得網域控制權限，因所有Windows都內建NTLM，所以未更新的系統都有此風險。
3. RDP重送攻擊漏洞是RDP在受限管理員(Restricted-Admin)模式下，允許降級使用NTLM驗證通訊協定進行身分驗證，導致攻擊者可利用NTLM驗證通訊協定相關漏洞(如搭配前述LDAP重送攻擊漏洞)進行攻擊，以取得網域控制權。只要在網域環境使用NTLM身分驗證服務都有可能存在這個問題。
4. 影響平臺：
   Windows 7 for 32-bit Systems Service Pack 1
   Windows 7 for x64-based Systems Service Pack 1
   Windows 8.1 for 32-bit systems
   Windows 8.1 for x64-based systems
   Windows RT 8.1
   Windows 10 for 32-bit Systems
   Windows 10 for x64-based Systems
   Windows 10 Version 1511 for 32-bit Systems
   Windows 10 Version 1511 for x64-based Systems
   Windows 10 Version 1607 for 32-bit Systems
   Windows 10 Version 1607 for x64-based Systems
   Windows 10 Version 1703 for 32-bit Systems
   Windows 10 Version 1703 for x64-based Systems
   Windows Server 2008 for 32-bit Systems Service Pack 2
   Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core安裝選項)
   Windows Server 2008 for Itanium-Based Systems Service Pack 2
   Windows Server 2008 for x64-based Systems Service Pack 2
   Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core安裝選項)
   Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
   Windows Server 2008 R2 for x64-based Systems Service Pack 1
   Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core安裝選項)
   Windows Server 2012
   Windows Server 2012 (Server Core安裝選項)
   Windows Server 2012 R2
   Windows Server 2012 R2 (Server Core安裝選項)

Windows Server 2016
Windows Server 2016 (Server Core安裝選項)

5. 建議措施：
    1. 目前微軟官方已針對此弱點釋出修復程式(https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8563)，請儘速進行更新。
6. 參考資料
    1. http://thehackernews.com/2017/07/windows-ntlm-security-flaw.html
    2. https://nvd.nist.gov/vuln/detail/CVE-2017-8563
    3. http://www.ithome.com.tw/news/115546
    4. https://blog.preempt.com/new-ldap-rdp-relay-vulnerabilities-in-ntlm

—- 計算機與通訊中心
網路系統組 敬啟