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-2017-0072	發布時間	Thu Jul 13 19:02:54 CST 2017
事件類型	漏洞預警	發現時間	Thu Jul 13 00:00:00 CST 2017
警訊名稱	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(CVE-2017-8563)，請儘速進行更新		
內容說明	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。 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。 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。		
影響平台	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)
影響等級	高
建議措施	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)，請各機關儘速進行更新。
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 https://blog.preempt.com/new-ldap-rdp-relay-vulnerabilities-in-ntlm

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