張貼日期：2019/05/15

【資安漏洞預警通知】微軟Windows遠端桌面服務存在安全漏洞(CVE-2019-0708)允許攻擊者遠端執行任意程式碼

主旨：【資安漏洞預警通知】微軟Windows遠端桌面服務存在安全漏洞(CVE-2019-0708)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:
  - 微軟Windows遠端桌面服務(Remote Desktop Services)在Windows Server 2008前之作業系統中稱為終端服務(Terminal Services)該服務允許使用者透過網路連線進行遠端操作電腦。
  - 研究人員發現遠端桌面服務存在安全漏洞(CVE-2019-0708)遠端攻擊者可對目標系統之遠端桌面服務發送特製請求，利用此漏洞進而遠端執行任意程式碼。
- 影響平台:
  - Windows XP
  - Windows 7
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2008 R2
- 建議措施:
  - 目前微軟官方已針對此弱點釋出更新程式，請儘速進行更新：
  1. Windows XP與Windows Server 2003作業系統雖已停止支援安全性更新，但微軟仍針對此漏洞釋出更新程式，請至下列連結進行更新：https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708
  2. 作業系統如為Windows 7Windows Server 2008及Windows Server 2008 R2請至下列連結進行更新：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
- 參考資料:
  1. https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/
  2. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

計算機與通訊中心
網路系統組 敬啟