張貼日期：2020/02/21

【資安攻擊預警】建議各單位勿開啟遠端桌面協定(RDP)以避免系統遭到入侵

主旨：建議各單位勿開啟遠端桌面協定(RDP)以避免系統遭到入侵

說明：

- 內容說明
  - 轉發國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202002-0558
  - 近期學術網路內發現仍有大量電腦疑似開啟Microsoft Windows遠端桌面服務(Remote Desktop Services(簡稱RDP)預設埠「3389」，因去年遠端桌面服務(RDP)已被通報存在下述安全漏洞，故建議各單位勿開啟遠端桌面協定(RDP)以避免系統遭到入侵。
    1. [TACERT-ANA-2019092008094646]研究人員發現遠端桌面服務存在安全漏洞(CVE-2019-1181、CVE-2019-1182、CVE-2019-1222及CVE-2019-1226)可讓未經身分驗證的遠端攻擊者，透過對目標系統的遠端桌面服務發送特製請求，在不需使用者進行任何操作互動之情況下，達到遠端執行任意程式碼之危害。
    2. [TACERT-ANA-2019051502053333]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。
  - Microsoft Windows遠端桌面服務(Remote Desktop Services)亦即在Windows Server 2008及更早版本中所稱之終端服務(Terminal Services)該服務允許使用者透過網路連線來遠端操作電腦或虛擬機。
- 影響平台: 開啟遠端桌面服務的系統
- 建議措施:
  1. 建議單位關閉遠端桌面(RDP)服務。
  2. 定期修補作業系統漏洞。
  3. 如果確實需要開啟此項服務，建議利用防火牆來限制來源端，設定僅允許管理者的主機可登入，而不要對外完全開放。
- 參考資料:
  1. https://thehackernews.com/2019/08/windows-rdp-wormable-flaws.html
  2. https://www.ithome.com.tw/news/132413
  3. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1222
  4. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1226
  5. https://www.nccst.nat.gov.tw/VulnerabilityNewsDetail?lang=zh&seq=1441
  6. https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/
  7. 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

From:
http://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
http://net.nthu.edu.tw/netsys/mailing:announcement:20200221_01

Last update: **2020/02/21 10:09**