張貼日期：2019/09/20

【資安漏洞預警Microsoft Windows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)

主旨Microsoft Windows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)、允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新

說明：

- 內容說明：
  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。
  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。
- 影響平台：
  Windows 7
  Windows 8.1
  Windows 10
  Windows Server 2008 R2
  Windows Server 2012
  Windows Server 2012 R2
  Windows Server 2016
  Windows Server 2019
- 建議措施：
  Microsoft官方已針對此弱點釋出修補程式，並包含於8月份例行性累積更新中，各機關可聯絡設備維護廠商或參考各CVE對應的安全性公告，進行Windows更新
- 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/releasenotedetail/312890cc-3673-e911-a991-000d3a33a34d
  4. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1222
  5. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1226
  6. https://www.nccst.nat.gov.tw/VulnerabilityNewsDetail?lang=zh&seq=1441

計算機與通訊中心
網路系統組 敬啟

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

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20190920_01

Last update: **2019/09/20 11:08**