張貼日期：2022/04/22

【資安漏洞預警Windows作業系統存在高風險安全漏洞(CVE-2022-26809)請儘速確認並進行更新！

- 主旨說明Windows作業系統存在高風險安全漏洞(CVE-2022-26809)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：
  - 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202204-0651
  - 研究人員發現Windows作業系統存在高風險安全漏洞(CVE-2022-26809)攻擊者可將特別製作之遠端程序呼叫(Remote Procedure Call簡稱RPC)傳送至RPC主機，即可獲得與RPC服務相同之權限，進而於伺服器上遠端執行任意程式碼。
- 影響平台:
  - 受影響版本如下：
    - Windows 10 for 32-bit Systems
    - Windows 10 for x64-based Systems
    - Windows 10 Version 1607 for 32-bit Systems
    - Windows 10 Version 1607 for x64-based Systems
    - Windows 10 Version 1809 for 32-bit Systems
    - Windows 10 Version 1809 for ARM64-based Systems
    - Windows 10 Version 1809 for x64-based Systems
    - Windows 10 Version 1909 for 32-bit Systems
    - Windows 10 Version 1909 for ARM64-based Systems
    - Windows 10 Version 1909 for x64-based Systems
    - Windows 10 Version 20H2 for 32-bit Systems
    - Windows 10 Version 20H2 for ARM64-based Systems
    - Windows 10 Version 20H2 for x64-based Systems
    - Windows 10 Version 21H1 for 32-bit Systems
    - Windows 10 Version 21H1 for ARM64-based Systems
    - Windows 10 Version 21H1 for x64-based Systems
    - Windows 10 Version 21H2 for 32-bit Systems
    - Windows 10 Version 21H2 for ARM64-based Systems
    - Windows 10 Version 21H2 for x64-based Systems
    - Windows 11 for ARM64-based Systems
    - Windows 11 for x64-based Systems
    - 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 Server 2008 for 32-bit Systems Service Pack 2
    - Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
    - Windows Server 2008 for x64-based Systems Service Pack 2
    - Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
    - Windows Server 2008 R2 for x64-based Systems Service Pack 1

  - Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
  - Windows Server 2012
  - Windows Server 2012 (Server Core installation)
  - Windows Server 2012 R2 Windows Server 2012 R2
  - Windows Server 2012 R2 (Server Core installation)
  - Windows Server 2016
  - Windows Server 2016 (Server Core installation)
  - Windows Server 2019
  - Windows Server 2019 (Server Core installation)
  - Windows Server 2022
  - Windows Server 2022 (Server Core installation)
  - Windows Server, version 20H2 (Server Core Installation)
- 建議措施:
  1. 目前微軟官方已針對此漏洞釋出更新程式，請各機關聯絡維護廠商或參考下列網址進行更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26809
  2. 若無法更新若無法更新至最新版本，請參考微軟官方網頁之Mitigations一節，採取下列緩解措施：
     1. 關閉邊界防火牆的TCP 445埠。
     2. 參考下列官方指引保護SMB流量：https://docs.microsoft.com/zh-tw/windows-server/storage/file-server/smb-secure-traffic
- 參考資料:
  1. https://www.ithome.com.tw/news/150440
  2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26809

計算機與通訊中心
網路系統組 敬啟