張貼日期：2021/02/18

【資安漏洞預警】微軟Windows TCP/IP存在安全漏洞(CVE-2021-24074、CVE-2021-24094及CVE-2021-24086)請儘速確認並進行更新！

- 主旨說明：【資安漏洞預警】微軟Windows TCP/IP存在安全漏洞(CVE-2021-24074、CVE-2021-24094及CVE-2021-24086)、允許攻擊者遠端執行任意程式碼或造成服務阻斷，請儘速確認並進行更新！

- 內容說明：
  - 轉發 行政院國家資通安全會報技術服務中心 資安訊息警訊 NISAC-ANA-202102-0902
  - 研究人員發現微軟Windows TCP/IP存在安全漏洞 CVE-2021-24074、CVE-2021-24094及CVE-2021-24086、可能遭受以下攻擊：
    1. 遠端攻擊者可發送特製封包，利用CVE-2021-24074或CVE-2021-24094執行任意程式碼。
    2. 遠端攻擊者可發送特製封包，利用CVE-2021-24086造成服務阻斷。
- 影響平台:
  受影響之Windows作業系統包含用戶端及伺服器版本，版本如下:
  - Windows Server, version 20H2 (Server Core Installation)
  - Windows 10 Version 20H2 for ARM64-based Systems
  - Windows 10 Version 20H2 for 32-bit Systems
  - Windows 10 Version 20H2 for x64-based Systems
  - Windows Server, version 2004 (Server Core installation)
  - Windows 10 Version 2004 for x64-based Systems
  - Windows 10 Version 2004 for ARM64-based Systems
  - Windows 10 Version 2004 for 32-bit Systems
  - Windows Server, version 1909 (Server Core installation)
  - Windows 10 Version 1909 for ARM64-based Systems
  - Windows 10 Version 1909 for x64-based Systems
  - Windows 10 Version 1909 for 32-bit Systems
  - Windows Server 2012 R2 (Server Core installation)
  - Windows Server 2012 R2
  - Windows Server 2012 (Server Core installation)
  - Windows Server 2012
  - Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
  - Windows Server 2008 R2 for x64-based Systems Service Pack 1
  - Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
  - Windows Server 2008 for x64-based Systems Service Pack 2
  - Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
  - Windows Server 2008 for 32-bit Systems Service Pack 2
  - Windows RT 8.1
  - Windows 8.1 for x64-based systems
  - Windows 8.1 for 32-bit systems
  - Windows 7 for x64-based Systems Service Pack 1
  - Windows 7 for 32-bit Systems Service Pack 1

  - Windows Server 2016 (Server Core installation)
  - Windows Server 2016
  - Windows 10 Version 1607 for x64-based Systems
  - Windows 10 Version 1607 for 32-bit Systems
  - Windows 10 for x64-based Systems
  - Windows 10 for 32-bit Systems
  - Windows Server 2019 (Server Core installation)
  - Windows Server 2019
  - Windows 10 Version 1809 for ARM64-based Systems
  - Windows 10 Version 1809 for x64-based Systems
  - Windows 10 Version 1809 for 32-bit Systems
  - Windows 10 Version 1803 for ARM64-based Systems
  - Windows 10 Version 1803 for x64-based Systems
  - Windows 10 Version 1803 for 32-bit Systems
- 建議措施:
  1. 目前微軟官方已針對此漏洞釋出更新程式，請各機關聯絡設備維護廠商或參考以下建議進行更新：
     1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24094
     2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24074
     3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24086
  2. 若無法立即更新，可參考官網公告採取緩解措施，並建議經測試再做調整。
     1. CVE-2021-24074執行官網因應措施中之PowerShell指令，停用IPv4之鬆散來源路由，防止攻擊者進行弱點利用，參考連結如下：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24074
     2. CVE-2021-24086與CVE-2021-24094執行官網因應措施中之PowerShell指令，於邊界網路設備上停用IPv6分段，防止攻擊者進行弱點利用，參考連結如下：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24086 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24094
- 參考資料:
  1. https://msrc-blog.microsoft.com/2021/02/09/multiple-security-updates-affecting-tcp-ip/
  2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24094
  3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24074
  4. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24086
  5. https://unit42.paloaltonetworks.com/cve-2021-24074-patch-tuesday/
  6. https://www.ithome.com.tw/news/142717

計算機與通訊中心
網路系統組 敬啟