張貼日期：2024/03/12

【漏洞預警】Microsoft Windows存在高風險安全漏洞(CVE-2024-21338)請儘速確認並進行修補!

- 主旨說明：【漏洞預警】Microsoft Windows存在高風險安全漏洞(CVE-2024-21338)請儘速確認並進行修補!
- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-200-202403-00000053
  - 研究人員發現Microsoft Windows作業系統的AppLocker安全功能存在本機提權漏洞(CVE-2024-21338)允許完成身分鑑別的本機端攻擊者，利用此漏洞提升至系統權限。該漏洞目前已遭駭客利用，請儘速確認並進行修補。
- 影響平台：
  - 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 21H2 for 32-bit Systems
  - Windows 10 Version 21H2 for ARM64-based Systems
  - Windows 10 Version 21H2 for x64-based Systems
  - Windows 10 Version 22H2 for 32-bit Systems
  - Windows 10 Version 22H2 for ARM64-based Systems
  - Windows 10 Version 22H2 for x64-based Systems
  - Windows 11 version 21H2 for ARM64-based Systems
  - Windows 11 version 21H2 for x64-based Systems
  - Windows 11 Version 22H2 for ARM64-based Systems
  - Windows 11 Version 22H2 for x64-based Systems
  - Windows 11 Version 23H2 for ARM64-based Systems
  - Windows 11 Version 23H2 for x64-based Systems
  - Windows Server 2019
  - Windows Server 2019 (Server Core installation)
  - Windows Server 2022
  - Windows Server 2022 (Server Core installation)
  - Windows Server 2022, 23H2 Edition (Server Core installation)
- 建議措施：
  - 官方已針對漏洞釋出修復更新，請參考以下網址確認修補資訊：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21338
- 參考資料：
  - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21338

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:20240312_01

Last update: **2024/03/12 13:50**