張貼日期：2025/10/29

【漏洞預警Windows SMB存在高風險安全漏洞(CVE-2025-33073)請儘速確認並進行修補

- 主旨說明:【漏洞預警Windows SMB存在高風險安全漏洞(CVE-2025-33073)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-200-202510-00000308
  - 研究人員發現Windows SMB用戶端存在NTLM反射(NTLM Reflection)漏洞(CVE-2025-33073)，取得一般使用者權限之遠端攻擊者，可透過執行惡意腳本，迫使SMB用戶端與攻擊者控制之SMB伺服器連線並進行身分鑑別，由於SMB用戶端在驗證階段存在缺陷，攻擊者可藉此繞過安全檢核以提升至系統權限，進而控制用戶端系統。該漏洞已遭駭客利用，請儘速確認並進行修補。
- 影響平台:
  - Windows Server 2025 (Server Core installation)
  - Windows Server 2025
  - Windows Server 2022, 23H2 Edition (Server Core installation)
  - Windows Server 2022 (Server Core installation)
  - Windows Server 2022
  - Windows Server 2019 (Server Core installation)
  - Windows Server 2019
  - Windows Server 2016 (Server Core installation)
  - Windows Server 2016
  - 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 11 Version 24H2 for x64-based Systems
  - Windows 11 Version 24H2 for ARM64-based Systems
  - Windows 11 Version 23H2 for x64-based Systems
  - Windows 11 Version 23H2 for ARM64-based Systems
  - Windows 11 Version 22H2 for x64-based Systems
  - Windows 11 Version 22H2 for ARM64-based Systems
  - Windows 10 Version 22H2 for x64-based Systems
  - Windows 10 Version 22H2 for ARM64-based Systems
  - Windows 10 Version 22H2 for 32-bit Systems
  - Windows 10 Version 21H2 for x64-based Systems
  - Windows 10 Version 21H2 for ARM64-based Systems
  - Windows 10 Version 21H2 for 32-bit Systems

    - Windows 10 Version 1809 for x64-based Systems
    - Windows 10 Version 1809 for 32-bit Systems
    - 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
- 建議措施:
    - 官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下：
      https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33073
- 參考資料:
    1. https://nvd.nist.gov/vuln/detail/CVE-2025-33073
    2. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2025-33073
    3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33073
    4. https://www.vicarius.io/vsociety/posts/cve-2025-33073-mitigation-script-improper-access-control-in-windows-smb-affects-microsoft-products

---

計算機與通訊中心
網路系統組 敬啟