

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2025102901104040	發佈時間	2025-10-29 13:18:40
事故類型	ANA-漏洞預警	發現時間	2025-10-29 13:18:40
影響等級	中		
[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。 情資分享等級: WHITE (情資內容為可公開揭露之資訊) 此訊息僅發送到「區縣市網路中心」，煩請貴單位協助轉發與通知轄下各單位知悉			
[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>