

張貼日期：2024/06/26

【漏洞預警】Windows Error Reporting Service 存在高風險安全漏洞(CVE-2024-26169)請儘速確認並進行修補！

- 主旨說明Windows Error Reporting Service存在高風險安全漏洞(CVE-2024-26169)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-200-202406-00000194
 - 研究人員發現Windows Error Reporting Service存在本地提權(Local Privilege Escalation)漏洞(CVE-2024-26169)已取得一般權限之本機端攻擊者可利用此漏洞提升至管理者權限。該漏洞已遭駭客利用，請儘速確認並進行修補。
- 影響平台:
 - 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 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 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 2022, 23H2 Edition (Server Core installation)
- 建議措施:
 - 官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下：<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26169>
- 參考資料:
 1. <https://nvd.nist.gov/vuln/detail/CVE-2024-26169>
 2. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26169>

3. <https://vulcan.io/blog/how-to-fix-cve-2024-26169/>

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/announcement:20240626_01



Last update: **2024/06/26 14:31**