

張貼日期：2026/08/07

【漏洞預警】Microsoft Excel存在高風險安全漏洞(CVE-2026-62870)請儘速確認並進行修補

- 主旨說明：【漏洞預警】Microsoft Excel存在高風險安全漏洞(CVE-2026-62870)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 資安訊息警訊 NISAC-200-202608-00000002
 - 研究人員發現Microsoft Excel存在使用釋放後記憶體(Use After Free)漏洞(CVE-2026-62870)未經身分鑑別之遠端攻擊者可利用此漏洞執行任意程式碼，請儘速確認並進行修補。
- 影響平台：
 - Microsoft 365 Apps for Enterprise for 32-bit Systems
 - Microsoft 365 Apps for Enterprise for 64-bit Systems
 - Microsoft Excel 2016 (32-bit edition) 16.0.5561.1001(不含)以前版本
 - Microsoft Excel 2016 (64-bit edition) 16.0.5561.1001(不含)以前版本
 - Microsoft Office 2019 for 32-bit editions
 - Microsoft Office 2019 for 64-bit editions
 - Microsoft Office LTSC 2021 for 32-bit editions
 - Microsoft Office LTSC 2021 for 64-bit editions
 - Microsoft Office LTSC 2024 for 32-bit editions
 - Microsoft Office LTSC 2024 for 64-bit editions
- 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-2026-62870>
- 參考資料：
 - <https://nvd.nist.gov/vuln/detail/CVE-2026-62870>
 - <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62870>

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/mailling:announcement:20260807_26

Last update: **2026/08/07 10:09**