

Date Posted: 2026/08/07

□Vulnerability Alert□High-Risk Security Vulnerability in Microsoft Excel (CVE-2026-62870); Please Confirm and Patch Promptly

- Subject: □Vulnerability Alert□High-Risk Security Vulnerability in Microsoft Excel (CVE-2026-62870); Please Confirm and Patch Promptly
- Description:
 - Forwarded Security Alert from National Information Sharing and Analysis Center (NISAC) NISAC-200-202608-00000002
 - Researchers have discovered a Use After Free vulnerability (CVE-2026-62870) in Microsoft Excel. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary code. Please confirm and apply patches as soon as possible.
- Affected Platforms:
 - Microsoft 365 Apps for Enterprise for 32-bit Systems
 - Microsoft 365 Apps for Enterprise for 64-bit Systems
 - Microsoft Excel 2016 (32-bit edition) versions prior to 16.0.5561.1001
 - Microsoft Excel 2016 (64-bit edition) versions prior to 16.0.5561.1001
 - 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
- Recommendations:
 - The vendor has released security patches for this vulnerability. Please refer to the official advisory to perform updates:
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62870>
- Reference Information:
 1. <https://nvd.nist.gov/vuln/detail/CVE-2026-62870>
 2. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62870>

Computer and Communication Center
Network Systems Division

From:

<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260807_26



Last update: **2026/08/07 10:11**