

張貼日期：2026/05/29

【漏洞預警】CISA新增10個已知遭駭客利用之漏洞至KEV目錄(2026/05/18-2026/05/24)

- 主旨說明: 【漏洞預警】CISA新增10個已知遭駭客利用之漏洞至KEV目錄(2026/05/18-2026/05/24)
- 內容說明:
 - 轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-200-202605-00000014
 - [CVE-2008-4250]Microsoft Windows Buffer Overflow Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用:未知】Microsoft Windows的Windows Server Service中存在緩衝區溢位漏洞，遠端攻擊者可透過特製的RPC請求，在路徑正規化過程中觸發緩衝區溢位，進而執行任意程式碼。
 - [CVE-2009-1537]Microsoft DirectX NULL Byte Overwrite Vulnerability (CVSS v3.1: 8.8)
 - 【是否遭勒索軟體利用:未知】Microsoft DirectX 中的 DirectShow 元件 quartz.dll 內的 QuickTime Movie Parser Filter 存在NULL 位元組覆寫漏洞。遠端攻擊者可透過特製的QuickTime媒體檔案觸發此漏洞，進而執行任意程式碼。
 - [CVE-2009-3459]Adobe Acrobat and Reader Heap-Based Buffer Overflow Vulnerability (CVSS v3.1: 8.8)
 - 【是否遭勒索軟體利用:未知】Adobe Acrobat and Reader 存在堆積型緩衝區溢位漏洞。遠端攻擊者可透過特製的PDF檔案觸發記憶體損毀，進而執行任意程式碼。
 - [CVE-2010-0249]Microsoft Internet Explorer Use-After-Free Vulnerability (CVSS v3.1: 8.8)
 - 【是否遭勒索軟體利用:未知】Microsoft Internet Explorer存在使用釋放後記憶體漏洞。遠端攻擊者可透過存取與已刪除物件相關聯的指標，進而執行任意程式碼。
 - [CVE-2010-0806]Microsoft Internet Explorer Use-After-Free Vulnerability (CVSS v3.1: 8.8)
 - 【是否遭勒索軟體利用:未知】Microsoft Internet Explorer 存在使用釋放後記憶體漏洞。遠端攻擊者可透過在物件刪除後存取無效指標的方式利用此漏洞，進而執行任意程式碼。
 - [CVE-2026-41091]Microsoft Defender Link Following Vulnerability (CVSS v3.1: 7.8)
 - 【是否遭勒索軟體利用:未知】Microsoft Defender 存在連結追蹤漏洞，允許已授權的攻擊者在本機提升權限。
 - [CVE-2026-45498]Microsoft Defender Denial of Service Vulnerability (CVSS v3.1: 4.0)
 - 【是否遭勒索軟體利用:未知】Microsoft Defender 存在未明確說明的漏洞，可能導致服務阻斷。
 - [CVE-2025-34291]Langflow Origin Validation Error Vulnerability (CVSS v3.1: 8.8)
 - 【是否遭勒索軟體利用:未知】Langflow存在來源驗證錯誤漏洞。由於其CORS設定過於寬鬆，並且refreshtoken的cookie設定為SameSite=None，攻擊者可能藉此存取需要身份驗證的端點，進而執行任意程式碼，最終取得系統完整控制權。
 - [CVE-2026-34926]Trend Micro Apex One (On-Premise) Directory Traversal Vulnerability (CVSS v3.1: 6.7)
 - 【是否遭勒索軟體利用:未知】Trend Micro Apex One (on-premise) 存在目錄遍歷漏洞，可能允許經預先驗證的本地攻擊者修改伺服器上的關鍵資料表，進而注入惡意程式碼並下發至受管端點設備。
 - [CVE-2026-9082]Drupal Core SQL Injection Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用:未知】Drupal Core 存在SQL注入漏洞。攻擊者可透過資料庫抽象 API 發送特製請求，藉此實現權限提升及遠端程式碼執行。
- 影響平台:
 - [CVE-2008-4250]請參考官方所列的影響版本
<https://learn.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067>

- [CVE-2009-1537]請參考官方所列的影響版本
<https://learn.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-028>
- [CVE-2009-3459]請參考官方所列的影響版本
<https://helpx.adobe.com/security/security-bulletin.html>
- [CVE-2010-0249]請參考官方所列的影響版本
<https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-002>
- [CVE-2010-0806]請參考官方所列的影響版本
<https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-018>
- [CVE-2026-41091]請參考官方所列的影響版本
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41091>
- [CVE-2026-45498]請參考官方所列的影響版本
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45498>
- [CVE-2025-34291] Langflow 1.6.9(含)之前的版本
- [CVE-2026-34926]請參考官方所列的影響版本
<https://success.trendmicro.com/en-US/solution/KA-0023430>
- [CVE-2026-9082]請參考官方所列的影響版本 <https://www.drupal.org/sa-core-2026-004>
- 建議措施:
 - [CVE-2008-4250] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://learn.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067>
 - [CVE-2009-1537] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://learn.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-028>
 - [CVE-2009-3459] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://helpx.adobe.com/security/security-bulletin.html>
 - [CVE-2010-0249] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-002>
 - [CVE-2010-0806] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-018>
 - [CVE-2026-41091] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41091>
 - [CVE-2026-45498] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45498>
 - [CVE-2025-34291] 對應產品升級至以下版本(或更高) Langflow 1.7.0
 - [CVE-2026-34926] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://success.trendmicro.com/en-US/solution/KA-0023430>
 - [CVE-2026-9082] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://www.drupal.org/sa-core-2026-004>

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:20260529_21



Last update: **2026/05/29 09:28**