Posting Date: 2026/05/29

【Vulnerability Alert】CISA Adds 10 Known Exploited Vulnerabilities to KEV Catalog (2026/05/18-2026/05/24)

- Subject: 【Vulnerability Alert】CISA Adds 10 Known Exploited Vulnerabilities to KEV Catalog (2026/05/18-2026/05/24)

- Description:
  - Forwarded from Taiwan Computer Emergency Response Team / Coordination Center Security Alert TWCERTCC-200-202605-00000014
  - 【CVE-2008-4250】Microsoft Windows Buffer Overflow Vulnerability (CVSS v3.1: 9.8)
  - 【Known Exploited by Ransomware: Unknown】 A buffer overflow vulnerability exists in the Windows Server Service of Microsoft Windows. Remote attackers can trigger a buffer overflow during the path normalization process via a specially crafted RPC request, thereby executing arbitrary code.
  - 【CVE-2009-1537】Microsoft DirectX NULL Byte Overwrite Vulnerability (CVSS v3.1: 8.8)
  - 【Known Exploited by Ransomware: Unknown】 A NULL byte overwrite vulnerability exists within the QuickTime Movie Parser Filter in the DirectShow component (quartz.dll) of Microsoft DirectX. Remote attackers can trigger this vulnerability via a specially crafted QuickTime media file, thereby executing arbitrary code.
  - 【CVE-2009-3459】Adobe Acrobat and Reader Heap-Based Buffer Overflow Vulnerability (CVSS v3.1: 8.8)
  - 【Known Exploited by Ransomware: Unknown】 A heap-based buffer overflow vulnerability exists in Adobe Acrobat and Reader. Remote attackers can trigger memory corruption via a specially crafted PDF file, thereby executing arbitrary code.
  - 【CVE-2010-0249】Microsoft Internet Explorer Use-After-Free Vulnerability (CVSS v3.1: 8.8)
  - 【Known Exploited by Ransomware: Unknown】 A use-after-free vulnerability exists in Microsoft Internet Explorer. Remote attackers can execute arbitrary code by accessing pointers associated with deleted objects.
  - 【CVE-2010-0806】Microsoft Internet Explorer Use-After-Free Vulnerability (CVSS v3.1: 8.8)
  - 【Known Exploited by Ransomware: Unknown】 A use-after-free vulnerability exists in Microsoft Internet Explorer. Remote attackers can exploit this vulnerability by accessing an invalid pointer after an object has been deleted, thereby executing arbitrary code.
  - 【CVE-2026-41091】Microsoft Defender Link Following Vulnerability (CVSS v3.1: 7.8)
  - 【Known Exploited by Ransomware: Unknown】 A link following vulnerability exists in Microsoft Defender, allowing an authorized attacker to elevate privileges locally.
  - 【CVE-2026-45498】Microsoft Defender Denial of Service Vulnerability (CVSS v3.1: 4.0)
  - 【Known Exploited by Ransomware: Unknown】 An unspecified vulnerability exists in Microsoft Defender, which could result in a denial of service.
  - 【CVE-2025-34291】Langflow Origin Validation Error Vulnerability (CVSS v3.1: 8.8)
  - 【Known Exploited by Ransomware: Unknown】 An origin validation error vulnerability exists in Langflow. Due to its overly permissive CORS settings and the refresh token cookie being set to SameSite=None, an attacker could potentially access authenticated endpoints, thereby executing arbitrary code and ultimately gaining full control of the

system.
    - 【CVE-2026-34926】Trend Micro Apex One (On-Premise) Directory Traversal Vulnerability (CVSS v3.1: 6.7)
    - 【Known Exploited by Ransomware: Unknown】 A directory traversal vulnerability exists in Trend Micro Apex One (on-premise), which could allow a pre-authenticated local attacker to modify critical data tables on the server, thereby injecting malicious code and deploying it to managed endpoint devices.
    - 【CVE-2026-9082】Drupal Core SQL Injection Vulnerability (CVSS v3.1: 9.8)
    - 【Known Exploited by Ransomware: Unknown】 An SQL injection vulnerability exists in Drupal Core. Attackers can send specially crafted requests via the database abstraction API to achieve privilege escalation and remote code execution.
- Affected Platforms:
    - 【CVE-2008-4250】 Please refer to the affected versions listed officially: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067
    - 【CVE-2009-1537】 Please refer to the affected versions listed officially: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-028
    - 【CVE-2009-3459】 Please refer to the affected versions listed officially: https://helpx.adobe.com/security/security-bulletin.html
    - 【CVE-2010-0249】 Please refer to the affected versions listed officially: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-002
    - 【CVE-2010-0806】 Please refer to the affected versions listed officially: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-018
    - 【CVE-2026-41091】 Please refer to the affected versions listed officially: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41091
    - 【CVE-2026-45498】 Please refer to the affected versions listed officially: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45498
    - 【CVE-2025-34291】 Langflow versions 1.6.9 and earlier
    - 【CVE-2026-34926】 Please refer to the affected versions listed officially: https://success.trendmicro.com/en-US/solution/KA-0023430
    - 【CVE-2026-9082】 Please refer to the affected versions listed officially: https://www.drupal.org/sa-core-2026-004
- Recommended Actions:
    - 【CVE-2008-4250】 The vendor has released patches for this vulnerability, please update to the relevant version: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067
    - 【CVE-2009-1537】 The vendor has released patches for this vulnerability, please update to the relevant version: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-028
    - 【CVE-2009-3459】 The vendor has released patches for this vulnerability, please update to the relevant version: https://helpx.adobe.com/security/security-bulletin.html
    - 【CVE-2010-0249】 The vendor has released patches for this vulnerability, please update to the relevant version: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-002
    - 【CVE-2010-0806】 The vendor has released patches for this vulnerability, please update to the relevant version: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-018
    - 【CVE-2026-41091】 The vendor has released patches for this vulnerability, please update to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41091
    - 【CVE-2026-45498】 The vendor has released patches for this vulnerability, please update

to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45498
- CVE-2025-34291 Upgrade the corresponding product to the following version (or higher): Langflow 1.7.0
- CVE-2026-34926 The vendor has released patches for this vulnerability, please update to the relevant version: https://success.trendmicro.com/en-US/solution/KA-0023430
- CVE-2026-9082 The vendor has released patches for this vulnerability, please update to the relevant version: https://www.drupal.org/sa-core-2026-004

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:20260529_21

Last update: **2026/05/29 09:43**