Posting Date: 2026/07/17

【Vulnerability Alert】CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2026/07/06-2026/07/12)

- Subject: 【Vulnerability Alert】CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2026/07/06-2026/07/12)

- Description:
  - Forwarded from the Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) security alert TWCERTCC-200-202607-00000006.
  - 【CVE-2026-48908】JoomShaper SP Page Builder Unrestricted Upload of File with Dangerous Type Vulnerability (CVSS v3.1: 9.8)
  - 【Whether exploited by ransomware: Unknown】 JoomShaper SP Page Builder contains an unrestricted upload of file with dangerous type vulnerability, allowing unauthenticated users to upload arbitrary files, which can ultimately lead to PHP code being uploaded and executed.
  - 【CVE-2026-55255】Langflow Authorization Bypass Through User-Controlled Key Vulnerability (CVSS v3.1: 8.4)
  - 【Whether exploited by ransomware: Unknown】 Langflow contains an authorization bypass vulnerability, allowing authenticated attackers to specify the victim's workflow ID in requests, thereby executing any workflow belonging to other users.
  - 【CVE-2026-56290】Joomlack Page Builder Improper Access Control Vulnerability (CVSS v3.1: 9.8)
  - 【Whether exploited by ransomware: Unknown】 Joomlack Page Builder contains an improper access control vulnerability, which could allow attackers to achieve remote code execution through unauthenticated arbitrary file uploads.
  - 【CVE-2026-48282】Adobe ColdFusion Path Traversal Vulnerability (CVSS v3.1: 10.0)
  - 【Whether exploited by ransomware: Unknown】 Adobe ColdFusion contains a path traversal vulnerability, which could result in arbitrary code execution under the privileges of the current user.
  - 【CVE-2026-56291】Balbooa Forms Unrestricted Upload of File with Dangerous Type Vulnerability (CVSS v3.1: 9.8)
  - 【Whether exploited by ransomware: Unknown】 Balbooa Forms contains an unrestricted upload of file with dangerous type vulnerability, allowing unauthenticated arbitrary file uploads, leading to remote code execution.
  - 【CVE-2026-48939】iCagenda Unrestricted Upload of File with Dangerous Type Vulnerability (CVSS v3.1: 9.8)
  - 【Whether exploited by ransomware: Unknown】 iCagenda contains an unrestricted upload of file with dangerous type vulnerability. Attackers can exploit the file attachment feature to upload arbitrary files, ultimately resulting in PHP code being uploaded and executed.
- Affected Platforms:
  - 【CVE-2026-48908】Please refer to the listed affected versions: https://mysites.guru/blog/sp-page-builder-zero-day-uploadcustomicon-rce/
  - 【CVE-2026-55255】Please refer to the official listed affected versions:

https://github.com/langflow-ai/langflow/security/advisories/GHSA-qrpv-q767-xqq2
  - CVE-2026-56290Please refer to the listed affected versions: https://mysites.guru/blog/pagebuilderck-unauthenticated-file-upload-rce/
  - CVE-2026-48282Please refer to the official listed affected versions: https://helpx.adobe.com/security/products/coldfusion/apsb26-68.html
  - CVE-2026-56291Please refer to the listed affected versions: https://mysites.guru/blog/balbooa-forms-unauthenticated-file-upload-flaw/
  - CVE-2026-48939Please refer to the listed affected versions: https://mysites.guru/blog/icagenda-zero-day-file-upload-rce/
- Recommended Actions:
  - CVE-2026-48908 A security update has been released to address this vulnerability. Please update to the relevant version: https://mysites.guru/blog/sp-page-builder-zero-day-uploadcustomicon-rce/
  - CVE-2026-55255 The official vendor has released a security update to address this vulnerability. Please update to the relevant version: https://github.com/langflow-ai/langflow/security/advisories/GHSA-qrpv-q767-xqq2
  - CVE-2026-56290 A security update has been released to address this vulnerability. Please update to the relevant version: https://mysites.guru/blog/pagebuilderck-unauthenticated-file-upload-rce/
  - CVE-2026-48282 The official vendor has released a security update to address this vulnerability. Please update to the relevant version: https://helpx.adobe.com/security/products/coldfusion/apsb26-68.html
  - CVE-2026-56291 A security update has been released to address this vulnerability. Please update to the relevant version: https://mysites.guru/blog/balbooa-forms-unauthenticated-file-upload-flaw/
  - CVE-2026-48939 A security update has been released to address this vulnerability. Please update to the relevant version: https://mysites.guru/blog/icagenda-zero-day-file-upload-rce/

Computer and Communication Center
Network Systems Division Sincerely

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260717_24

Last update: **2026/07/17 11:54**