Posted Date: 2026/07/28 \

【Vulnerability Alert】CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2026/07/20-2026/07/26)

- Subject: 【Vulnerability Alert】CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2026/07/20-2026/07/26)

\

- Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center Cybersecurity Alert Information TWCERTCC-200-202607-00000012
  - 【CVE-2026-60137】WordPress Core SQL Injection Vulnerability (CVSS v3.1: 5.9)
  - 【Known Ransomware Use: Unknown】 WordPress Core contains an SQL injection vulnerability when a plugin or theme passes untrusted input to the affected parameter. This vulnerability can be chained with CVE-2026-63030, allowing an unauthenticated attacker to achieve remote code execution in default WordPress installations.
  - 【CVE-2026-63030】WordPress Core Interpretation Conflict Vulnerability (CVSS v3.1: 9.8)
  - 【Known Ransomware Use: Unknown】 WordPress Core contains an Interpretation Conflict vulnerability that may allow attackers to execute SQL injection and achieve remote code execution. This vulnerability can be chained with CVE-2026-60137.
  - 【CVE-2026-0770】Langflow Inclusion of Functionality from Untrusted Control Sphere Vulnerability (CVSS v3.1: 9.8)
  - 【Known Ransomware Use: Unknown】 Langflow contains an Inclusion of Functionality from Untrusted Control Sphere vulnerability that allows remote attackers to execute arbitrary code on affected installations.
  - 【CVE-2021-27137】DD-WRT Stack-Based Buffer Overflow Vulnerability (CVSS v3.1: 8.1)
  - 【Known Ransomware Use: Unknown】 DD-WRT contains a stack-based buffer overflow vulnerability. An unauthenticated attacker can exploit this vulnerability to overflow an internal buffer used by UPnP, thereby triggering a code execution vulnerability.
  - 【CVE-2026-16232】Check Point SmartConsole Improper Authentication Vulnerability (CVSS v3.1: 9.1)
  - 【Known Ransomware Use: Unknown】 Check Point SmartConsole contains an improper authentication vulnerability. An unauthenticated remote attacker can exploit this vulnerability to obtain an application login token and authenticate with full administrator privileges.
  - 【CVE-2026-50522】Microsoft SharePoint Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.8)
  - 【Known Ransomware Use: Unknown】 Microsoft SharePoint contains a deserialization of untrusted data vulnerability. An unauthorized attacker could exploit this vulnerability to execute arbitrary code over the network.
- Affected Systems:
  - 【CVE-2026-60137】 Please refer to the official listed affected versions https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-fpp7-x2x2-2mjf
  - 【CVE-2026-63030】 Please refer to the official listed affected versions

https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-ff9f-jf42-662q
  - CVE-2026-0770 Langflow version 1.7.3 and prior
  - CVE-2021-27137 DD-WRT versions prior to 45724
  - CVE-2026-16232 Please refer to the official listed affected versions https://support.checkpoint.com/results/sk/sk185169/
  - CVE-2026-50522 Please refer to the official listed affected versions https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50522
- Recommended Actions:
  - CVE-2026-60137 The vendor has released patch updates for the vulnerability; please update to the relevant versions https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-fpp7-x2x2-2mjf
  - CVE-2026-63030 The vendor has released patch updates for the vulnerability; please update to the relevant versions https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-ff9f-jf42-662q
  - CVE-2026-0770 Currently, the vendor has not released a corresponding patch; it is recommended to update to other unaffected versions https://github.com/langflow-ai/langflow
  - CVE-2021-27137 The vendor has released patch updates for the vulnerability; please update to the relevant versions https://svn.dd-wrt.com/changeset/45724
  - CVE-2026-16232 The vendor has released patch updates for the vulnerability; please update to the relevant versions https://support.checkpoint.com/results/sk/sk185169/
  - CVE-2026-50522 The vendor has released patch updates for the vulnerability; please update to the relevant versions https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50522

Computer and Communication Center \ Network System Division

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260728_21

Last update: **2026/07/28 14:08**