Date Posted: 2026/06/04

【Vulnerability Alert】CISA Adds 5 Known Exploited Vulnerabilities to KEV Catalog (2026/05/25-2026/05/31)

- Subject: 【Vulnerability Alert】CISA Adds 5 Known Exploited Vulnerabilities to KEV Catalog (2026/05/25-2026/05/31)

- Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Cyber Security Alert TWCERTCC-200-202606-00000001
  - 【CVE-2026-48172】LiteSpeed cPanel Plugin Privilege Escalation Vulnerability (CVSS v3.1: 9.8)
  - 【Ransomware Exploitation: Unknown】 A privilege escalation vulnerability exists in LiteSpeed cPanel Plugin. This vulnerability can be triggered via the user-side cPanel plugin, allowing any cPanel user account to abuse this vulnerability and execute arbitrary scripts with root privileges.
  - 【CVE-2026-48027】Nx Console Embedded Malicious Code Vulnerability (CVSS v3.1: 9.8)
  - 【Ransomware Exploitation: Known】 An embedded malicious code vulnerability exists in Nx Console. Attackers leverage this to publish malicious versions of Nx Console. The affected extensions download an obfuscated malicious payload that can steal credentials from multiple sources in disk and memory.
  - 【CVE-2026-45321】TanStack Unspecified Vulnerability (CVSS v31: 9.6)
  - 【Ransomware Exploitation: Known】 An unspecified vulnerability exists in TanStack, allowing attackers to publish malicious versions of the package to the npm Registry and utilize trusted identities to distribute credential-stealing malware.
  - 【CVE-2026-8398】Daemon Tools Lite Embedded Malicious Code Vulnerability (CVSS v3.1: 9.8)
  - 【Ransomware Exploitation: Unknown】 An unspecified vulnerability exists in Daemon Tools, causing a high impact on confidentiality, integrity, and availability.
  - 【CVE-2026-0257】Palo Alto Networks PAN-OS Authentication Bypass Vulnerability (CVSS v3.1: 9.1)
  - 【Ransomware Exploitation: Unknown】 An authentication bypass vulnerability exists in Palo Alto Networks PAN-OS, allowing attackers to bypass security restrictions and establish unauthorized VPN connections.
- Affected Platforms:
  - 【CVE-2026-48172】Please refer to the affected versions listed by the official website: https://blog.litespeedtech.com/2026/05/21/security-update-for-litespeed-cpanel-plugin/
  - 【CVE-2026-48027】Please refer to the affected versions listed by the official website: https://nx.dev/blog/nx-console-v18-95-0-postmortem#indicators-of-compromise
  - 【CVE-2026-45321】Please refer to the affected versions listed by the official website: https://github.com/TanStack/router/security/advisories/GHSA-g7cv-rxg3-hmpx
  - 【CVE-2026-8398】Please refer to the affected versions listed by the official website: https://blog.daemon-tools.cc/post/security-incident
  - 【CVE-2026-0257】Please refer to the affected versions listed by the official website:

https://security.paloaltonetworks.com/CVE-2026-0257

- Recommended Actions:
  - □CVE-2026-48172□ The vendor has released a security patch for this vulnerability. Please update to the relevant version: https://blog.litespeedtech.com/2026/05/21/security-update-for-litespeed-cpanel-plugin/
  - □CVE-2026-48027□ The vendor has released a security patch for this vulnerability. Please update to the relevant version: https://nx.dev/blog/nx-console-v18-95-0-postmortem#indicators-of-compromise
  - □CVE-2026-45321□ The vendor has released a security patch for this vulnerability. Please update to the relevant version: https://github.com/TanStack/router/security/advisories/GHSA-g7cv-rxg3-hmpx
  - □CVE-2026-8398□ The vendor has released a security patch for this vulnerability. Please update to the relevant version: https://blog.daemon-tools.cc/post/security-incident
  - □CVE-2026-0257□ The vendor has released a security patch for this vulnerability. Please update to the relevant version: https://security.paloaltonetworks.com/CVE-2026-0257

Computer and Communication Center
Network Systems Division