Posting Date: 2026/06/24

Vulnerability Alert CISA Adds 4 Known Exploited Vulnerabilities to KEV Catalog (2026/06/15-2026/06/21)

- Subject: Vulnerability Alert CISA Adds 4 Known Exploited Vulnerabilities to KEV Catalog (2026/06/15-2026/06/21)

- Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center Security Alert TWCERTCC-200-202606-00000017
  - CVE-2026-54420 LiteSpeed cPanel Plugin UNIX Symbolic Link (Symlink) Following Vulnerability (CVSS v3.1: 8.5)
  - Ransomware Use: Unknown A UNIX symbolic link following vulnerability exists in the LiteSpeed cPanel plugin. On shared hosting servers running CloudLinux/CageFS, users with FTP or Web Shell access could exploit this vulnerability to perform unauthorized operations.
  - CVE-2026-20262 Cisco Catalyst SD-WAN Manager Directory or Path Traversal Vulnerability (CVSS v3.1: 6.5)
  - Ransomware Use: Unknown A directory or path traversal vulnerability exists in Cisco Catalyst SD-WAN Manager. An authenticated, remote attacker could exploit this vulnerability to create files or overwrite arbitrary files in the file system of an affected system.
  - CVE-2026-48907 Widget Factory Joomla Content Editor Improper Access Control Vulnerability (CVSS v3.1: 9.8)
  - Ransomware Use: Unknown An improper access control vulnerability exists in Widget Factory Joomla Content Editor, which could allow an unauthenticated user to upload and execute PHP code by creating a new editor profile.
  - CVE-2026-20253 Splunk Enterprise Missing Authentication for Critical Function Vulnerability (CVSS v3.1: 9.8)
  - Ransomware Use: Unknown A missing authentication for critical function vulnerability exists in Splunk Enterprise. An unauthenticated user could create or truncate arbitrary files via the PostgreSQL Sidecar service endpoint.
- Affected Platforms:
  - CVE-2026-54420 Please refer to the affected versions listed by the official source: https://blog.litespeedtech.com/2026/06/01/security-update-for-litespeed-cpanel-plugin-2/
  - CVE-2026-20262 Please refer to the affected versions listed by the official source: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfw-c2rZvQ
  - CVE-2026-48907 Please refer to the affected versions listed by the official source: https://www.joomlacontenteditor.net/news/jce-security-update-and-a-free-patch-for-older-sites
  - CVE-2026-20253 Please refer to the affected versions listed by the official source: https://advisory.splunk.com/advisories/SVD-2026-0603
- Recommended Actions:

- □CVE-2026-54420□ The official source has released a fix for the vulnerability; please update to the relevant version: https://blog.litespeedtech.com/2026/06/01/security-update-for-litespeed-cpanel-plugin-2/
- □CVE-2026-20262□ The official source has released a fix for the vulnerability; please update to the relevant version: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfw-c2rZvQ
- □CVE-2026-48907□ The official source has released a fix for the vulnerability; please update to the relevant version: https://www.joomlacontenteditor.net/news/jce-security-update-and-a-free-patch-for-older-sites
- □CVE-2026-20253□ The official source has released a fix for the vulnerability; please update to the relevant version: https://advisory.splunk.com/advisories/SVD-2026-0603

Computer and Communication Center
Network Systems Division