Post Date: 2026/05/13

【Vulnerability Alert】CISA Adds 14 Known Exploited Vulnerabilities to KEV Catalog (2026/04/20-2026/04/26) (Part 1)

- Subject: 【Vulnerability Alert】CISA Adds 14 Known Exploited Vulnerabilities to KEV Catalog (2026/04/20-2026/04/26) (Part 1)

- Description:
  - Forwarded from Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert: TWCERTCC-200-202604-00000027
  - 【CVE-2026-20122】Cisco Catalyst SD-WAN Manager Incorrect Use of Privileged APIs Vulnerability (CVSS v3.1: 5.4)
  - 【Ransomware Exploitation: Unknown】 Cisco Catalyst SD-WAN Manager contains an incorrect use of privileged APIs vulnerability. An attacker can exploit this by uploading malicious files to the local file system. Successful exploitation allows an attacker to overwrite arbitrary files on the affected system and obtain vmanage user privileges.
  - 【CVE-2026-20133】Cisco Catalyst SD-WAN Manager Exposure of Sensitive Information to an Unauthorized Actor Vulnerability (CVSS v3.1: 6.5)
  - 【Ransomware Exploitation: Unknown】 Cisco Catalyst SD-WAN Manager contains a vulnerability where sensitive information is exposed to unauthorized actors, which may allow a remote attacker to view sensitive information on the affected system.
  - 【CVE-2025-2749】Kentico Xperience Path Traversal Vulnerability (CVSS v3.1: 7.2)
  - 【Ransomware Exploitation: Unknown】 Kentico Xperience contains a path traversal vulnerability that could allow an authenticated user's Staging Sync Server to upload arbitrary data to a relative path location.
  - 【CVE-2023-27351】PaperCut NG/MF Improper Authentication Vulnerability (CVSS v3.1: 8.2)
  - 【Ransomware Exploitation: Known】 PaperCut NG/MF contains an improper authentication vulnerability that could allow a remote attacker to bypass authentication for the affected installation via the SecurityRequestFilter class.
  - 【CVE-2025-48700】Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability (CVSS v3.1: 6.1)
  - 【Ransomware Exploitation: Unknown】 Synacor Zimbra Collaboration Suite (ZCS) contains a cross-site scripting vulnerability that could allow an attacker to execute arbitrary JavaScript within a user's session, leading to unauthorized access to sensitive information.
  - 【CVE-2026-20128】Cisco Catalyst SD-WAN Manager Storing Passwords in a Recoverable Format Vulnerability (CVSS v3.1: 7.5)
  - 【Ransomware Exploitation: Unknown】 Cisco Catalyst SD-WAN Manager contains a vulnerability where passwords are stored in a recoverable format, allowing an authenticated local attacker with low-level user privileges to access the DCA user's credentials file in the file system, thereby obtaining DCA user privileges.
  - 【CVE-2025-32975】Quest KACE Systems Management Appliance (SMA) Improper Authentication Vulnerability (CVSS v3.1: 10.0)
  - 【Ransomware Exploitation: Unknown】 Quest KACE Systems Management Appliance

(SMA) contains an improper authentication vulnerability that could allow an attacker to impersonate a legitimate user without valid credentials.

- Affected Platforms:
  - CVE-2026-20122 Please refer to the official list of affected versions: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v
  - CVE-2026-20133 Please refer to the official list of affected versions: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v
  - CVE-2025-2749 Kentico Xperience versions 13.0.178 (inclusive) and earlier.
  - CVE-2023-27351 Please refer to the official list of affected versions: https://www.papercut.com/kb/Main/PO-1216-and-PO-1219
  - CVE-2025-48700 Please refer to the official list of affected versions: https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories
  - CVE-2026-20128 Please refer to the official list of affected versions: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v
  - CVE-2025-32975 Please refer to the official list of affected versions: https://support.quest.com/kb/4379499/quest-response-to-kace-sma-vulnerabilities-cve-2025-32975-cve-2025-32976-cve-2025-32977-cve-2025-32978
- Recommended Actions:
  - CVE-2026-20122 Official fix updates have been released; please update to the relevant version: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v
  - CVE-2026-20133 Official fix updates have been released; please update to the relevant version: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v
  - CVE-2025-2749 Official fix updates have been released; please update to the relevant version: https://devnet.kentico.com/download/hotfixes
  - CVE-2023-27351 Official fix updates have been released; please update to the relevant version: https://www.papercut.com/kb/Main/PO-1216-and-PO-1219
  - CVE-2025-48700 Official fix updates have been released; please update to the relevant version: https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories
  - CVE-2026-20128 Official fix updates have been released; please update to the relevant version: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v
  - CVE-2025-32975 Official fix updates have been released; please update to the relevant version: https://support.quest.com/kb/4379499/quest-response-to-kace-sma-vulnerabilities-cve-2025-32975-cve-2025-32976-cve-2025-32977-cve-2025-32978

Computer and Communication Center
Network Systems Division