La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) añadió el lunes ocho nuevas vulnerabilidades a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV), incluyendo tres fallos que afectan a Cisco Catalyst SD-WAN Manager, citando evidencias de explotación activa.

La lista de vulnerabilidades es la siguiente:

- CVE-2023-27351 (puntuación CVSS: 8.2) – Una vulnerabilidad de autenticación incorrecta en PaperCut NG/MF que podría permitir a un atacante eludir los mecanismos de autenticación en instalaciones afectadas mediante la clase SecurityRequestFilter.
- CVE-2024-27199 (puntuación CVSS: 7.3) – Una vulnerabilidad de recorrido de rutas relativas en JetBrains TeamCity que podría permitir a un atacante ejecutar acciones administrativas limitadas.
- CVE-2025-2749 (puntuación CVSS: 7.2) – Una vulnerabilidad de *path traversal* en Kentico Xperience que podría permitir a un usuario autenticado usar el servidor Staging Sync para cargar datos arbitrarios en rutas relativas.
- CVE-2025-32975 (puntuación CVSS: 10.0) – Una falla de autenticación deficiente en Quest KACE Systems Management Appliance (SMA) que podría permitir a un atacante suplantar usuarios legítimos sin credenciales válidas.
- CVE-2025-48700 (puntuación CVSS: 6.1) – Una vulnerabilidad de *cross-site scripting* en Synacor Zimbra Collaboration Suite (ZCS) que podría permitir ejecutar JavaScript arbitrario dentro de la sesión del usuario, provocando acceso no autorizado a información sensible.
- CVE-2026-20122 (puntuación CVSS: 5.4) – Un uso indebido de APIs privilegiadas en Cisco Catalyst SD-WAN Manager que podría permitir a un atacante cargar y sobrescribir archivos arbitrarios en el sistema afectado y obtener privilegios de usuario vmanage.
- CVE-2026-20128 (puntuación CVSS: 7.5) – Un almacenamiento de contraseñas en formato recuperable en Cisco Catalyst SD-WAN Manager que podría permitir a un atacante local autenticado escalar privilegios accediendo a un archivo de credenciales del usuario DCA.

- CVE-2026-20133 (puntuación CVSS: 6.5) – Una vulnerabilidad de exposición de información sensible en Cisco Catalyst SD-WAN Manager que podría permitir a atacantes remotos visualizar datos confidenciales en sistemas afectados.

Cabe destacar que CISA ya había incorporado CVE-2024-27198, otra vulnerabilidad que afecta a versiones locales de JetBrains TeamCity, al catálogo KEV en marzo de 2024. Por ahora, no está claro si ambas fallas están siendo explotadas conjuntamente ni si corresponden al mismo actor de amenazas.

En cuanto a CVE-2023-27351, su explotación fue atribuida al grupo Lace Tempest en abril de 2023, en campañas relacionadas con la distribución de ransomware de las familias Cl0p y LockBit.

Respecto a CVE-2025-32975, Arctic Wolf indicó que detectó a actores desconocidos aprovechando esta vulnerabilidad para atacar sistemas SMA sin parches hasta finales del mes pasado, aunque los objetivos finales de la campaña aún no están definidos.

Según el Equipo de Respuesta a Emergencias Informáticas de Ucrania (CERT-UA), un actor identificado como UAC-0233 ha explotado dos vulnerabilidades en ZCS (CVE-2025-48700 y CVE-2025-66376) en ataques dirigidos a entidades ucranianas desde septiembre de 2025, permitiendo la ejecución de código arbitrario sin interacción del usuario. CVE-2025-66376 fue añadida al catálogo KEV de CISA a mediados de marzo de 2026.

«Tras comprometer con éxito los sistemas, los atacantes obtuvieron acceso al contenido de los buzones, incluyendo correspondencia almacenada en archivos TGZ, códigos de respaldo de autenticación multifactor, contraseñas de aplicaciones y el directorio global de direcciones,» indicó CERT-UA en su informe del segundo semestre de 2025 publicado a inicios de este mes. *«Esta actividad se rastrea bajo el identificador UAC-0250.»*

Por su parte, Cisco también confirmó que tuvo conocimiento de la explotación de CVE-2026-20122 y CVE-2026-20128 en marzo de 2026. Sin embargo, la compañía aún no ha actualizado su aviso para reflejar el uso activo de CVE-2026-20133.

Ante la evidencia de explotación activa, se ha recomendado a las agencias del Federal Civilian Executive Branch (FCEB) corregir las tres vulnerabilidades de Cisco antes del 23 de abril de 2026, y el resto antes del 4 de mayo de 2026.