Se han revelado dos vulnerabilidades de seguridad de alta gravedad en Composer, un gestor de paquetes para PHP, que, si se explotan con éxito, podrían permitir la ejecución arbitraria de comandos.

Las fallas han sido identificadas como errores de inyección de comandos que afectan al controlador Perforce VCS (software de control de versiones). A continuación se detallan ambas vulnerabilidades –

CVE-2026-40176 (puntuación CVSS: 7.8) – Una vulnerabilidad por validación inadecuada de entradas que podría permitir a un atacante, al controlar la configuración de un repositorio en un archivo composer.json malicioso que declare un repositorio Perforce VCS, inyectar comandos arbitrarios, provocando su ejecución en el contexto del usuario que ejecuta Composer.

CVE-2026-40261 (puntuación CVSS: 8.8) – Una vulnerabilidad de validación insuficiente derivada de un escape incorrecto que podría permitir a un atacante insertar comandos arbitrarios mediante una referencia de origen manipulada que incluya metacaracteres de shell.

En ambos escenarios, Composer ejecutaría estos comandos inyectados incluso si Perforce VCS no está instalado, según indicaron los responsables en un aviso oficial.

Las vulnerabilidades impactan a las siguientes versiones –

> = 2.3, < 2.9.6 (corregido en la versión 2.9.6)
> = 2.0, < 2.2.27 (corregido en la versión 2.2.27)

Si no es posible aplicar los parches de inmediato, se recomienda revisar los archivos composer.json antes de ejecutar Composer y comprobar que los campos relacionados con Perforce contienen valores válidos. También se aconseja utilizar únicamente repositorios de Composer de confianza, ejecutar comandos de Composer en proyectos provenientes de

fuentes seguras y evitar instalar dependencias usando la opción «–prefer-dist» o la configuración «preferred-install: dist».

Composer informó que analizó Packagist.org y no encontró indicios de que estas vulnerabilidades hayan sido explotadas por actores maliciosos mediante la publicación de paquetes con información de Perforce manipulada. Se espera además el lanzamiento de una nueva versión para los clientes de Private Packagist Self-Hosted.

«Como medida preventiva, la publicación de metadatos de origen de Perforce ha sido deshabilitada en Packagist.org desde el viernes 10 de abril de 2026», indicó la compañía. «Se recomienda actualizar Composer de inmediato en todos los casos».