Progress Software ha publicado actualizaciones para corregir dos vulnerabilidades de seguridad en MOVEit Automation, incluyendo un fallo crítico que podría permitir la evasión de autenticación.

MOVEit Automation (anteriormente conocido como Central) es una solución segura de transferencia de archivos gestionada (MFT) basada en servidor, utilizada para programar y automatizar flujos de movimiento de archivos en entornos empresariales sin necesidad de scripts personalizados.

Las vulnerabilidades en cuestión son CVE-2026-4670 (puntuación CVSS: 9.8), una falla que permite omitir la autenticación, y CVE-2026-5174 (puntuación CVSS: 7.7), un problema de validación incorrecta de entradas que podría facilitar la escalada de privilegios.

«Las vulnerabilidades críticas y de alta severidad en MOVEit Automation pueden permitir la evasión de autenticación y la escalada de privilegios a través de las interfaces del puerto de comandos del backend del servicio,» señaló Progress Software en un aviso. *«Su explotación podría derivar en accesos no autorizados, control administrativo y exposición de datos.»*

Las versiones afectadas son las siguientes:

- MOVEit Automation <= 2025.1.4 (corregido en MOVEit Automation 2025.1.5)
- MOVEit Automation <= 2025.0.8 (corregido en MOVEit Automation 2025.0.9)
- MOVEit Automation <= 2024.1.7 (corregido en MOVEit Automation 2024.1.8)

Los investigadores de Airbus SecLab, Anaïs Gantet, Delphine Gourdou, Quentin Liddell y Matteo Ricordeau, fueron quienes descubrieron y reportaron ambas vulnerabilidades. No existen soluciones temporales que mitiguen estos problemas.

Aunque Progress Software no ha indicado que estas fallas estén siendo explotadas activamente, es fundamental que los usuarios apliquen las actualizaciones lo antes posible para garantizar una protección adecuada, especialmente considerando que vulnerabilidades previas en MOVEit Transfer han sido aprovechadas por grupos de ransomware como Cl0p.