Progress Software ha anunciado el descubrimiento y la solución de una vulnerabilidad crítica de inyección SQL en MOVEit Transfer, un software popular utilizado para la transferencia segura de archivos. Además, Progress Software ha corregido dos vulnerabilidades de alta gravedad adicionales.

La vulnerabilidad de inyección SQL identificada, catalogada como CVE-2023-36934, podría permitir potencialmente a atacantes no autenticados obtener acceso no autorizado a la base de datos de MOVEit Transfer.

Las vulnerabilidades de inyección SQL son una conocida y peligrosa falla de seguridad que permite a los atacantes manipular bases de datos y ejecutar cualquier código que deseen. Los atacantes pueden enviar cargas diseñadas específicamente a ciertos puntos finales de la aplicación afectada, lo que podría cambiar o exponer datos sensibles en la base de datos.

La razón por la cual CVE-2023-36934 es tan crítica radica en su capacidad de ser explotada sin necesidad de iniciar sesión. Esto significa que incluso atacantes sin credenciales válidas podrían potencialmente aprovechar la vulnerabilidad. Sin embargo, hasta el momento no se han reportado informes de esta vulnerabilidad en particular siendo utilizada activamente por atacantes.

Este descubrimiento surge después de una serie de ciberataques recientes que utilizaron una vulnerabilidad de inyección SQL diferente (CVE-2023-34362) para atacar MOVEit Transfer con ransomware Clop. Estos ataques resultaron en robo de datos y extorsión de dinero a las organizaciones afectadas.

Esta última actualización de seguridad de Progress Software también aborda dos vulnerabilidades de alta gravedad adicionales: CVE-2023-36932 y CVE-2023-36933.

CVE-2023-36932 es una falla de inyección SQL que puede ser aprovechada por atacantes que hayan iniciado sesión para obtener acceso no autorizado a la base de datos de MOVEit Transfer. Por otro lado, CVE-2023-36933 es una vulnerabilidad que permite a los atacantes cerrar abruptamente el programa MOVEit Transfer.

Investigadores de HackerOne y la Iniciativa Zero Day de Trend Micro informaron de manera responsable a Progress Software sobre estas vulnerabilidades.

Estas vulnerabilidades afectan a varias versiones de MOVEit Transfer, incluyendo 12.1.10 y versiones anteriores, 13.0.8 y versiones anteriores, 13.1.6 y versiones anteriores, 14.0.6 y versiones anteriores, 14.1.7 y versiones anteriores, y 15.0.3 y versiones anteriores.

Progress Software ha puesto a disposición las actualizaciones necesarias para todas las versiones principales de MOVEit Transfer. Se recomienda encarecidamente a los usuarios que actualicen a la última versión de MOVEit Transfer para reducir los riesgos asociados con estas vulnerabilidades.