Se ha revelado recientemente una falla de seguridad crítica que afecta a Progress Software MOVEit Transfer, y ya se están observando intentos de explotación poco después de que se hicieran públicos los detalles del error.

La vulnerabilidad, identificada como CVE-2024-5806 (con una puntuación CVSS de 9.1), se refiere a una omisión de autenticación que afecta a las siguientes versiones:

- Desde 2023.0.0 hasta 2023.0.10
- Desde 2023.1.0 hasta 2023.1.5, y
- Desde 2024.0.0 hasta 2024.0.1

> *«Una vulnerabilidad de autenticación incorrecta en Progress MOVEit Transfer (módulo SFTP) puede llevar a una omisión de autenticación»*, indicó la compañía en un aviso publicado el martes.

Progress también ha abordado otra vulnerabilidad crítica relacionada con la omisión de autenticación en SFTP (CVE-2024-5805, con una puntuación CVSS de 9.1) que afecta a la versión 2024.0.0 de MOVEit Gateway.

La explotación exitosa de estas fallas podría permitir a los atacantes eludir la autenticación SFTP y obtener acceso a los sistemas MOVEit Transfer y Gateway.

watchTowr Labs ha publicado detalles técnicos adicionales sobre CVE-2024-5806, con los investigadores de seguridad Aliz Hammond y Sina Kheirkhah señalando que podría ser utilizada para hacerse pasar por cualquier usuario en el servidor.

La empresa de ciberseguridad describió la falla como compuesta por dos vulnerabilidades separadas, una en Progress MOVEit y la otra en la biblioteca IPWorks SSH.

> *«Si bien la vulnerabilidad más devastadora, la capacidad de hacerse pasar por*

> *usuarios arbitrarios, es exclusiva de MOVEit, la vulnerabilidad de autenticación forzada menos impactante (pero aún muy real) probablemente afecte a todas las aplicaciones que utilizan el servidor IPWorks SSH»,* indicaron los investigadores.

Progress Software afirmó que la deficiencia en el componente de terceros *«aumenta el riesgo del problema original»* si no se corrige, instando a los clientes a seguir los siguientes dos pasos:

1. Bloquear el acceso RDP entrante público a los servidores MOVEit Transfer.
2. Limitar el acceso saliente solo a puntos finales de confianza conocidos desde los servidores MOVEit Transfer.

Según Rapid7, hay tres requisitos previos para aprovechar CVE-2024-5806: Los atacantes necesitan conocer un nombre de usuario existente, la cuenta objetivo puede autenticarse de forma remota y el servicio SFTP es accesible públicamente a través de Internet.

A partir del 25 de junio, los datos recopilados por Censys muestran que hay aproximadamente 2,700 instancias de MOVEit Transfer en línea, la mayoría ubicadas en EE. UU., Reino Unido, Alemania, Países Bajos, Canadá, Suiza, Australia, Francia, Irlanda y Dinamarca.

Con otro problema crítico en MOVEit Transfer ampliamente explotado en una serie de ataques de ransomware Cl0p el año pasado (CVE-2023-34362, con una puntuación CVSS de 9.8), es crucial que los usuarios actualicen rápidamente a las versiones más recientes.

Este desarrollo se produce cuando la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) reveló que su Herramienta de Evaluación de Seguridad Química (CSAT) fue atacada a principios de enero por un actor de amenazas desconocido que aprovechó fallas de seguridad en el dispositivo Ivanti Connect Secure (ICS) (CVE-2023-46805, CVE-2024-21887 y CVE-2024-21893).

> *«Esta intrusión puede haber resultado en el acceso no autorizado potencial a encuestas Top-Screen, Evaluaciones de Vulnerabilidad de Seguridad, Planes de Seguridad del Sitio, presentaciones del Programa de Seguridad del Personal (PSP) y cuentas de usuario de CSAT»*, dijo la agencia, añadiendo que no encontró evidencia de exfiltración de datos.