La Agencia de Seguridad Cibernética e Infraestructura de Estados Unidos (CISA) ha añadido una seria vulnerabilidad en el controlador de zonas de almacenamiento de Citrix ShareFile a su catálogo de Vulnerabilidades Conocidas Explotadas (KEV), basándose en pruebas de explotación activa en la vida real.

Identificada como CVE-2023-24489 (puntuación CVSS: 9.8), esta debilidad ha sido descrita como un fallo de control de acceso inadecuado que, si se aprovecha exitosamente, podría permitir a un atacante no autenticado comprometer instancias vulnerables de forma remota.

El problema radica en la forma en que ShareFile maneja las operaciones criptográficas, permitiendo a los adversarios subir archivos arbitrarios, lo que resulta en una ejecución de código remota.

> *«Cualquier versión actualmente soportada del controlador de zonas de almacenamiento de ShareFile gestionado por el cliente antes de la versión 5.11.24 se ve afectada por esta vulnerabilidad»,* señaló Citrix en un aviso emitido en junio. Dylan Pindur de Assetnote ha sido reconocido por descubrir y reportar este problema.

Es importante mencionar que los primeros signos de explotación de esta vulnerabilidad surgieron a finales de julio de 2023.

La identidad de los actores de amenazas detrás de estos ataques es desconocida, aunque el grupo de ransomware Cl0p ha mostrado interés en aprovechar vulnerabilidades zero-day en soluciones de transferencia de archivos gestionadas como Accellion FTA, SolarWinds Serv-U, GoAnywhere MFT y Progress MOVEit Transfer en los últimos años.

La firma de inteligencia en amenazas GreyNoise informó sobre un incremento significativo en los intentos de explotación dirigidos a esta vulnerabilidad, con hasta 75 direcciones IP únicas registradas solamente el 15 de agosto de 2023.

> *«CVE-2023-24489 es un error criptográfico en el Controlador de Zonas de Almacenamiento de Citrix ShareFile, una aplicación web .NET que opera bajo IIS»*, comentó GreyNoise.

> *«La aplicación utiliza cifrado AES en modo CBC y relleno PKCS7, pero no valida adecuadamente los datos descifrados. Esta falla permite a los atacantes generar un relleno válido y ejecutar su ataque, lo que conduce a la carga no autenticada de archivos arbitrarios y a la ejecución de código remoto.»*

Se ha requerido a las agencias del Sector Ejecutivo Civil Federal (FCEB) aplicar soluciones proporcionadas por el proveedor para remediar esta vulnerabilidad antes del 6 de septiembre de 2023.

Este acontecimiento ocurre en un contexto donde se han generado alarmas de seguridad debido a la explotación activa de CVE-2023-3519, una vulnerabilidad crítica que afecta al producto NetScaler de Citrix, utilizada para desplegar shells web PHP en dispositivos comprometidos y obtener acceso persistente.