Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CISA AGREGA FALLA DE CITRIX SHAREFILE AL CATÁLOGO KEV DEBIDO A ATAQUES

21/Agosto/2023

CONTENIDO

INTRODUCCIÓN

La Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA) ha agregado una falla de seguridad crítica en el controlador de zonas de almacenamiento Citrix ShareFile a su catálogo de vulnerabilidades explotadas conocidas (KEV), basándose en la evidencia de explotación activa en la naturaleza.

CISA AGREGA FALLA DE CITRIX SHAREFILE AL CATÁLOGO KEV DEBIDO A ATAQUES

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2023_08_21_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alto
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	21/08/2023
Es día cero (0 day):	Si

RESUMEN

Rastreado como CVE-2023-24489 (puntuación CVSS: 9.8), la deficiencia se ha descrito como un error de control de acceso incorrecto que, si se explota con éxito, podría permitir que un atacante no autenticado comprometa instancias vulnerables de forma remota.

El problema tiene sus raíces en el manejo de operaciones criptográficas de ShareFile, lo que permite a los adversarios cargar archivos arbitrarios, lo que resulta en la ejecución remota de código.

“Esta vulnerabilidad afecta a todas las versiones actualmente compatibles del controlador de zonas de almacenamiento ShareFile administrado por el cliente antes de la versión 5.11.24”, dijo Citrix en un aviso publicado en junio. Dylan Pindur de Assetnote ha sido acreditado por descubrir y reportar el problema.

Vale la pena señalar que los primeros signos de explotación de la vulnerabilidad surgieron hacia fines de julio de 2023.

Se desconoce la identidad de los actores de amenazas detrás de los ataques, aunque la pandilla de ransomware Cl0p ha tomado un interés particular en aprovechar los días cero en soluciones de

transferencia de archivos administrados como Accellion FTA, SolarWinds Serv-U, GoAnywhere MFT y Progress MOVEit Transfer en los últimos años.

La firma de inteligencia de amenazas GreyNoise dijo que observó un aumento significativo en los intentos de explotación dirigidos a la falla, con hasta 75 direcciones IP únicas registradas solo 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 se ejecuta bajo IIS", dijo GreyNoise.

"La aplicación utiliza cifrado AES con modo CBC y relleno PKCS7, pero no valida correctamente los datos descifrados. Este descuido permite a los atacantes generar relleno válido y ejecutar su ataque, lo que lleva a la carga de archivos arbitrarios no autenticados y a la ejecución remota de código".

Las agencias del Poder Ejecutivo Civil Federal (FCEB) han recibido el mandato de aplicar correcciones proporcionadas por el proveedor para remediar la vulnerabilidad antes del 6 de septiembre de 2023.

El desarrollo se produce cuando se han generado alarmas de seguridad sobre la explotación activa de CVE-2023-3519, una vulnerabilidad crítica que afecta al producto NetScaler de Citrix, para implementar shells web PHP en dispositivos comprometidos y obtener acceso persistente.

CVE ID	Productos afectados	Descripción	Requisitos previos	CWE	CVSS
CVE-2023-24489	Colaboración de contenido de Citrix	El control de recursos incorrecto permite un compromiso remoto no autenticado	Acceso de red al controlador de zonas de almacenamiento ShareFile	CWE-284	9.1

LO QUE SE DEBE HACER:
La versión más reciente del controlador de zonas de almacenamiento ShareFile está disponible en la siguiente ubicación:
https://www.citrix.com/downloads/sharefile/product-software/sharefile-storagezones-controller-511.html

Las instrucciones para actualizar el controlador de zonas de almacenamiento están aquí:
https://docs.sharefile.com/en-us/storage-zones-controller/5-0/upgrade.html

NOTA: Todas las versiones anteriores a la última versión 5.11.24 de los controladores de zonas de almacenamiento de ShareFile gestionados por el cliente han sido bloqueadas para proteger a nuestros clientes. Los clientes podrán restablecer el controlador de zonas de almacenamiento una vez que se aplique la actualización a la versión 5.11.24.

RECOMENDACIONES

Este problema se ha solucionado en las siguientes versiones del controlador de zonas de almacenamiento ShareFile administrado por el cliente:

- ShareFile Storage zones controller 5.11.24 y versiones posteriores

Los clientes deben actualizar a la versión fija.

NOTICIA COMPLETA

https://devel.group/blog/cisa-agrega-falla-de-citrix-sharefile-al-catalogo-kev-debido-a-ataques/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente