Kiteworks

GUÍA TÉCNICA

MOVEit: registro de vulnerabilidades de tres años

Historial de brechas, análisis de la arquitectura de seguridad, implicaciones regulatorias y la alternativa arquitectónica

En mayo de 2023, una vulnerabilidad crítica de inyección SQL en Progress MOVEit Transfer (CVE-2023-34362) se convirtió en el vehículo de una de las mayores brechas de datos en la cadena de suministro registradas. Tres años después, MOVEit ha acumulado al menos 11 CVE divulgadas en tres líneas de producto, incluidas cinco con una puntuación CVSS de la National Validation Database (NVD) de 9.0 o superior, y la plataforma sigue en ciclos de explotación activa. La divulgación del 30 de abril de 2026 de **CVE-2026-4670** (omisión de autenticación con CVSS 9.8) y **CVE-2026-5174** en MOVEit Automation marca la tercera oleada de vulnerabilidades críticas que afecta a la plataforma en tres años.

Este análisis en profundidad examina lo que el historial de MOVEit dice a los responsables de seguridad y cumplimiento sobre la arquitectura de la transferencia gestionada de archivos como categoría. El patrón es estructural -- una propiedad de plataformas que combinan una superficie expuesta a internet, infraestructura gestionada por el cliente, contenido sensible en reposo y una contención limitada cuando se descubre una vulnerabilidad. La respuesta arquitectónica no es un producto MFT diferente. Es un modelo completamente distinto.

Qué argumenta este informe

El patrón de vulnerabilidades de MOVEit no es una serie de mala suerte. Es el resultado predecible de una arquitectura que coloca una aplicación web expuesta a internet, un sistema operativo gestionado por el cliente, un backend SQL y un almacén de archivos sobre un único límite de confianza.

Cambiar de proveedor de MFT reinicia el ciclo de parches. Cambiar de arquitectura lo termina.

11+ CVE de MOVEit divulgadas en tres líneas de producto en tres años

5 con CVSS NVD de 9.0 o superior -- severidad crítica

1.440+ instancias de MOVEit Automation expuestas a internet en riesgo hoy

1

Registro de tres años

De un vistazo

2023

Cl0p explota MOVEit Transfer en masa. Más de 2.700 organizaciones, ~93 M de personas.

2024

Dos omisiones de autenticación con CVSS NVD 9.1. Código de explotación público el primer día.

2025

Escalada de privilegios en el módulo SFTP Shared Accounts.

2026

Omisión de autenticación con CVSS NVD 9.8 + escalada de privilegios en MOVEit Automation. Sin solución alternativa.

La explotación masiva de Cl0p en 2023 y las CVE posteriores

El 27 de mayo de 2023, el grupo de ransomware Cl0p comenzó la explotación masiva de CVE-2023-34362, una vulnerabilidad de inyección SQL con CVSS 9.8 en MOVEit Transfer. Progress lanzó un parche el 31 de mayo, pero en algunos casos Mandiant observó robo de datos **en cuestión de minutos tras el desarrollo del web shell** -- el parche llegó después de la mayor parte del daño. La cadena de ataque combinó inyección SQL en la aplicación web, una falla de deserialización que convirtió el token de sysadmin resultante en ejecución remota de código, y la ausencia de contención arquitectónica entre la aplicación y el almacenamiento subyacente de Azure Blob. Cl0p desplegó un web shell ASP.NET personalizado llamado LEMURLOOT, disfrazado como *human2.aspx*, que creó cuentas de administrador ocultas etiquetadas como “Health Check Service” y exfiltró datos mediante cabeceras HTTP personalizadas.

Cómo la cadena de ataque Cl0p de 2023 alcanzó los datos

1 Inyección SQL en la capa web

Inyección SQL no autenticada en la interfaz web pública de MOVEit Transfer -- la superficie requerida para el acceso de socios -- expuso tokens con alcance de sysadmin.

2 Deserialización hacia ejecución remota de código

Una falla de deserialización convirtió el token capturado en ejecución arbitraria de código en el host. La aplicación web y la base de datos ahora ejecutaban las instrucciones del atacante.

3 Web shell LEMURLOOT instalado

Un web shell ASP.NET personalizado (human2.aspx) creó cuentas de administrador ocultas llamadas “Health Check Service” y canalizó la exfiltración mediante cabeceras HTTP personalizadas.

4 Acceso directo al almacén de archivos

Ningún límite de capa separaba la aplicación del almacén de archivos ni de las credenciales de Azure Blob. Una vez dentro, el radio de impacto cubrió cada archivo del cliente que la plataforma alojaba.

Al cierre de 2023, la campaña había comprometido a más de 2.700 organizaciones y expuesto datos personales de aproximadamente 93,3 millones de personas. CISA estimó que más de 3.000 entidades de EE. UU. y más de 8.000 en todo el mundo se vieron afectadas cuando se incluyó la exposición aguas abajo -- más de cuatro de cada cinco organizaciones víctimas no tenían relación directa con Progress. En las seis semanas posteriores a la divulgación inicial, Progress identificó cinco CVE adicionales: CVE-2023-35036 (9 de junio), CVE-2023-35708 (15 de junio) y el service pack de julio que abordó CVE-2023-36932, CVE-2023-36933 y CVE-2023-36934 (CVSS 9.1 crítica).

Nombradas en las divulgaciones de Cl0p sobre MOVEit Transfer en 2023

BBC	British Airways	Departamento de Energía de EE. UU.	Universidad Johns Hopkins
Shell	Louisiana Airways	Oregon DMV	Maximus (11,3 M)
Welltok (10 M)	Delta Dental de CA (6,9 M)	CMS / WPS (3,1 M)	+ 2.700 más

El par de omisiones de autenticación de 2024

El 25 de junio de 2024, Progress divulgó **CVE-2024-5805** (omisión de autenticación crítica con CVSS 9.1 en MOVEit Gateway) y **CVE-2024-5806** (inicialmente CVSS 7.4, elevada a 9.1 crítica dos días después, cuando se divulgó una vulnerabilidad de la biblioteca de terceros IPWorks SSH). Ambas eran fallas de autenticación incorrecta en el módulo SFTP. La Shadowserver Foundation observó intentos de explotación contra CVE-2024-5806 a las pocas horas de la divulgación. WatchTowr Labs publicó código de prueba de concepto funcional el mismo día. La explotación solo requería un nombre de usuario válido, alcanzable mediante credential spraying contra el servicio SFTP.

“Los intentos de explotación llegaron en cuestión de horas tras la divulgación. El código de prueba de concepto funcional fue público ese mismo día. La explotación solo necesitaba un nombre de usuario válido.” -- Omisión de autenticación en MOVEit Gateway / Transfer -- junio de 2024

El problema de escalada de privilegios de 2025 y la divulgación de 2026

En 2025, Progress divulgó **CVE-2025-2324**, una vulnerabilidad de gestión incorrecta de privilegios en el módulo SFTP de MOVEit Transfer que afectaba a usuarios configurados como Shared Accounts. El aviso del 30 de abril de 2026 divulgó después **CVE-2026-4670** y **CVE-2026-5174** en MOVEit Automation, la línea de producto que automatiza y programa operaciones de MFT -- nóminas, reclamaciones sanitarias, transacciones financieras, presentaciones regulatorias. Shodan identificó más de 1.440 instancias de MOVEit Automation expuestas a internet en riesgo, incluidas 16 conectadas a gobiernos estatales y locales de EE. UU.

El patrón entre proveedores: cuatro vulnerabilidades MFT críticas en 18 meses

MOVEit es el ejemplo más cubierto, pero el patrón no es exclusivo de un proveedor. A lo largo de 2024 y 2025, cuatro plataformas MFT distintas publicaron vulnerabilidades de severidad crítica, cada una explotada en una breve ventana tras la divulgación pública.

Cleo	CrushFTP	Wing FTP	MOVEit
Dic. 2024	Mar. 2025	Jul. 2025	Abr. 2026
Explotación masiva de Cl0p; 300+ víctimas reivindicadas en transporte, manufactura y alimentación.	Omisión de autenticación; la divulgación posterior de julio de 2025 permitió la toma completa del servidor.	RCE sin autenticación mediante inyección Lua; impacto de privilegios root/SYSTEM.	Omisión de autenticación con CVSS NVD 9.8 + escalada de privilegios en Automation. Sin solución alternativa.

Historial de CVE de MOVEit, 2023-2026

Año	CVE	Vector	CVSS NVD	Impacto
2023	CVE-2023-34362	Inyección SQL (Transfer)	9.8	Día cero de Cl0p; 2.700+ orgs, 93M+ personas
2023	CVE-2023-35036	Inyección SQL (Transfer)	Crítica	Seguimiento divulgado el 9 de junio
2023	CVE-2023-35708	Inyección SQL (Transfer)	Crítica	Seguimiento divulgado el 15 de junio
2023	CVE-2023-36932	Inyección SQL (Transfer)	Alta	Service pack de julio
2023	CVE-2023-36933	Excepción no controlada	Alta	Service pack de julio
2023	CVE-2023-36934	Inyección SQL (Transfer)	9.1	Service pack de julio
2024	CVE-2024-5805	Omisión de autenticación (Gateway SFTP)	9.1	Divulgada el 25 de junio; PoC el mismo día
2024	CVE-2024-5806	Omisión de autenticación (Transfer SFTP)	9.1	Explotación de Shadowserver en horas
2025	CVE-2025-2324	Escalada de privilegios (SFTP)	Alta	Módulo Shared Accounts
2026	CVE-2026-4670	Omisión de autenticación (Automation)	9.8	Aviso actual; sin solución alternativa
2026	CVE-2026-5174	Validación de entrada (Automation)	8.8	Encadenada con CVE-2026-4670

2

Por qué la arquitectura sigue fallando

MOVEit es un producto de transferencia gestionada de archivos típico de la categoría: una aplicación web ejecutándose sobre infraestructura Windows gestionada por el cliente, respaldada por una base de datos SQL Server, opcionalmente con un componente Gateway al frente y archivos en reposo en el sistema de archivos local o en Azure Blob Storage. Cuatro propiedades arquitectónicas se combinan para producir el patrón de CVE.

La lectura estructural

Cada una de las cuatro propiedades siguientes es normal para la categoría MFT. Combinadas en un único límite de confianza, producen el modo de fallo que documenta el historial de CVE.

1. Superficie de aplicación web expuesta a internet

La interfaz web pública es necesaria para el acceso de socios. Toda inyección SQL, omisión de autenticación o falla de validación de entrada divulgada alcanza la plataforma a través de esta superficie.

2. Infraestructura gestionada por el cliente

La seguridad depende de que el cliente refuerce correctamente Windows, IIS, SQL Server y la red. Cada configuración incorrecta es una posible CVE en el entorno operativo.

3. Sin contención una vez dentro

Una vez que un atacante tiene RCE, nada aísla la aplicación de la base de datos, del almacén de archivos ni de las credenciales de Azure Blob. El radio de impacto es total.

4. Ciclo de parches sin solución alternativa

Cada CVE divulgada ha requerido una actualización con instalador completo. Explotación observada en cuestión de horas tras la divulgación en múltiples casos. El ciclo se acumula.

3

Implicaciones regulatorias

Las plataformas MFT se sitúan en el punto de paso obligado del intercambio de datos para cargas reguladas: información de salud protegida bajo HIPAA, información no clasificada controlada bajo CMMC y DFARS, datos de titulares de tarjetas bajo PCI DSS, datos personales bajo GDPR y leyes estatales de privacidad, registros financieros bajo SOX y normas de la SEC. Cuando la plataforma MFT es el vehículo de la brecha, la exposición regulatoria recae en el cliente -- no en Progress. Cada divulgación de MOVEit también acorta la defensa regulatoria disponible: la campaña de Cl0p de 2023 fue un día cero, el par de omisiones de autenticación de 2024 se divulgó con código de explotación funcional el primer día, y la divulgación de 2026 tiene más de 1.440 instancias expuestas a internet en riesgo.

Régimen	Norma	Exposición	Detonante vinculado a MOVEit
EE. UU. federal	SEC Item 1.05 (dic. 2023)	Divulgación pública 8-K de incidente material en 4 días hábiles	La SEC abrió una investigación formal de Progress el 2 de octubre de 2023
EE. UU. sanidad	Regla de Seguridad de HIPAA 45 CFR §164.308	Estándar de salvaguardas razonables de OCR; sanciones civiles de hasta 2,1 M USD por tope anual por nivel de infracción	Brecha de CMS/WPS notificada a OCR que afectó a 3,1 M de personas
EE. UU. defensa	CMMC Nivel 2 / DFARS 252.204-7012	Evaluación C3PAO requerida; notificación de incidente al DoD en 72 horas	MFT expuesta a internet implica directamente SC.L2-3.13.1, SC.L2-3.13.5, AC.L2-3.1.20
UE	Artículo 32 del GDPR + NIS 2 (oct. 2024)	Hasta el 4 % del volumen global; alerta temprana en 24 h / notificación de incidente en 72 h	La ICO impuso una multa de 14 M £ a Capita en oct. 2025 citando el artículo 32
Australia	APP 11 + Privacy Amendment Act 2024	Hasta 50 M AUD o el 30 % del volumen ajustado por interferencias graves o reiteradas	Notificaciones OAIC NDB +25 % interanual en 2024; el procedimiento Medibank sienta precedente

“La pregunta del regulador no es si la brecha era previsible. Es si continuar operando la plataforma tras tres oleadas de vulnerabilidades críticas en tres años constituye una salvaguarda razonable.”

4

La alternativa arquitectónica

Cambiar MOVEit por otro producto MFT reinicia el reloj del ciclo de parches sin cambiar el modelo subyacente. La respuesta arquitectónica es una plataforma que consolida la superficie de intercambio de datos sobre un appliance virtual reforzado y monoinquilino, con un único motor de políticas, un único registro de auditoría y la seguridad como capacidad del producto en lugar de como carga de configuración del cliente.

Appliance virtual reforzado, no infraestructura gestionada por el cliente

Kiteworks se implementa como un appliance virtual reforzado con firewall de red, firewall de aplicaciones web y detección de intrusiones integrados, y un sistema operativo despojado mantenido por Kiteworks. Los clientes no configuran el sistema operativo, no gestionan la base de datos y no parchean la pila subyacente por separado. Las actualizaciones de sistema completo con un solo clic parchean todo el appliance -- aplicación, runtime, sistema operativo, bibliotecas -- en una sola operación coordinada.

Defensa en profundidad, demostrada

Durante el incidente de Log4Shell en diciembre de 2021, la puntuación CVSS NVD del sector para la falla subyacente de Log4j era de 10,0.

Los controles en capas de Kiteworks contuvieron la explotabilidad práctica de Log4Shell en nuestro entorno antes de que llegara el parche formal. La evaluación interna de Kiteworks estimó la explotabilidad residual en aproximadamente CVSS 4,0; esta cifra es una estimación interna, no una puntuación CVSS emitida oficialmente por NIST o la CVE Numbering Authority.

La defensa en profundidad no es teórica aquí -- es la razón por la que un CVSS NVD de 10 quedó contenido.

Aislamiento monoinquilino y cifrado FIPS 140-3

Cada implementación de Kiteworks es monoinquilina por diseño -- sin bases de datos, sistemas de archivos ni runtimes compartidos entre clientes. Internamente, una arquitectura por niveles aísla la capa web de la base de datos y del almacén de archivos, de modo que una capa de aplicación comprometida no puede consultar directamente la base de datos ni derivar claves a nivel de archivo. Los archivos en reposo están protegidos por dos capas de cifrado independientes (a nivel de archivo y a nivel de disco) mediante módulos criptográficos validados FIPS 140-3, con TLS 1.3 en tránsito y gestión de claves controlada por el cliente de forma opcional para cargas de soberanía.

Arquitectura de MOVEit vs. arquitectura de Kiteworks

Seis propiedades arquitectónicas diferencian a las dos plataformas. Cada una se corresponde directamente con uno de los modos de fallo documentados en el historial de MOVEit. Fecha de divulgación de la comparativa: 12 de mayo de 2026. La caracterización de MOVEit refleja la plataforma tal como la documenta Progress en la fecha del aviso del 30 de abril de 2026; las capacidades del producto y las opciones de implementación pueden cambiar en versiones posteriores de Progress.

Dimensión	Arquitectura de MOVEit	Arquitectura de Kiteworks
Infraestructura	Windows Server, IIS y SQL Server gestionados por el cliente; SO y red reforzados por el cliente	Appliance virtual reforzado mantenido por Kiteworks; firewall, WAF e IDS integrados; actualizaciones con un solo clic
Contención	La aplicación web tiene acceso directo a todos los archivos del cliente y a la base de datos	Arquitectura por niveles; el nivel web no puede acceder al almacén de archivos ni derivar claves a nivel de archivo
Protección de datos	Cifrado en la capa de aplicación; logs de aplicación; la integración con SIEM es responsabilidad del cliente	Cifrado FIPS 140-3 de doble capa (archivo + disco); registro de auditoría a prueba de manipulaciones; entrega SIEM en tiempo real
Acceso administrativo privilegiado	La consola de administración es el propio SO Windows, por lo que los administradores acceden al código del servidor y al sistema de archivos y pueden instalar aplicaciones. Los atacantes que obtengan acceso privilegiado a la consola pueden instalar su propio código para tareas como control remoto y exfiltración de datos.	Los administradores no tienen acceso al SO, al sistema de archivos, al código de la aplicación ni a la base de datos, que están totalmente dentro del appliance virtual reforzado. La consola de administración es una interfaz web con estrictos controles de acceso basados en roles (sistema, aplicación, soporte, personalizado); las capacidades de administración manipulan el sistema solo mediante llamadas API específicas, y los administradores no pueden instalar software en el appliance.
Gestión de usuarios	Utiliza la gestión de usuarios de Windows como gestión de usuarios de la aplicación. Según la configuración, el radio de impacto puede extenderse más allá del entorno de MOVEit.	Sistema de gestión de usuarios diseñado específicamente, totalmente separado de la gestión de usuarios del sistema operativo
Cadencia de parches	Tres oleadas críticas en tres años; sin soluciones alternativas; ventanas de cambio de emergencia	Evento rutinario de parche de proveedor; la explotabilidad práctica de Log4Shell fue contenida por controles en capas antes de que llegara el parche

Si opera MOVEit Automation hoy

Cuatro acciones que merece la pena emprender esta semana

- Aplique el parche para MOVEit Automation 2025.1.5, 2025.0.9 o 2024.1.8 utilizando el instalador completo -- Progress confirma que no hay solución alternativa para CVE-2026-4670 ni CVE-2026-5174.
- Inventaríe las instancias de Automation expuestas a internet y revise los registros de auditoría en busca de indicadores de compromiso en las interfaces del puerto de comandos del backend del servicio.
- Incluya una revisión arquitectónica en el próximo ciclo de planificación. La pregunta ya no es si parchear -- es si el modelo de plataforma sigue siendo defendible tras tres oleadas críticas en tres años.
- Hable con Kiteworks sobre una revisión arquitectónica de 30 minutos -- vea cómo un modelo de appliance reforzado y monoinquilino cambiaría el radio de impacto la próxima vez que aparezca una CVE de clase MFT.

Aviso legal

Este análisis se basa en avisos de seguridad divulgados públicamente, investigaciones de terceros y la evaluación arquitectónica de Kiteworks al 11 de mayo de 2026. Las características técnicas de los productos de terceros pueden cambiar. Este documento no constituye asesoramiento legal ni de seguridad.

Kiteworks

Mayo de 2026