Alerta Vulnerabilidad
Vulnerabilidad en MOVEit Automation

CSIRTSALUD-AV-202600506-45 **TLP: CLEAR**

Alerta ID:	045
Fecha del reporte:	06/05/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidad en MOVEit Automation
Herramienta de detección	N/A
Activo involucrado:	Sistemas internos, nube y terceros
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la vulnerabilidad crítica identificada como CVE-2026-4670 en Progress MOVEit Automation, la cual puede permitir un bypass de autenticación y, en consecuencia, el acceso no autorizado a plataformas empresariales utilizadas para la transferencia automatizada de archivos.

El propósito de esta alerta es que las organizaciones del sector salud determinen con prioridad si utilizan MOVEit Automation de manera directa o indirecta, ya sea en infraestructura propia, ambientes en la nube, servicios tercerizados, canales de intercambio con aliados estratégicos o soluciones tecnológicas integradas a sus procesos misionales. Esta validación debe incluir la revisión de inventarios tecnológicos, contratos con proveedores, servicios MFT, integraciones de intercambio de archivos, conectores con sistemas clínicos, repositorios documentales,

plataformas de facturación, canales de reporte obligatorio y flujos asociados a información de pacientes.

Asimismo, el objetivo es promover una respuesta preventiva y coordinada que permita reducir el riesgo de exposición, alteración, consulta indebida o extracción de información sensible, especialmente aquella relacionada con historias clínicas, resultados diagnósticos, autorizaciones, datos administrativos de pacientes, soportes de atención, información financiera asociada a servicios de salud y demás datos personales o clínicos protegidos por la normativa colombiana.

Descripción:

El 4 de mayo de 2026, medios especializados reportaron que Progress Software advirtió a sus clientes sobre una vulnerabilidad crítica en MOVEit Automation, una solución empresarial de Managed File Transfer —MFT— usada para automatizar transferencias de archivos entre servidores internos, servicios en la nube y socios externos.

La vulnerabilidad principal es CVE-2026-4670, calificada con severidad CVSS 9.8 —Crítica—. Según NVD, corresponde a una falla de authentication bypass by primary weakness, asociada a CWE-305, y puede permitir omitir controles de autenticación.

Progress también corrigió una segunda vulnerabilidad, CVE-2026-5174, de severidad alta, relacionada con validación incorrecta de entradas y posible escalamiento de privilegios. The Hacker News reportó que ambas vulnerabilidades podrían permitir acceso no autorizado, control administrativo y exposición de datos mediante interfaces del puerto de comandos del backend del servicio.

Consecuencias de la explotación

La explotación exitosa de la vulnerabilidad **CVE-2026-4670** en Progress MOVEit Automation podría tener consecuencias graves para las entidades del sector salud, tanto a nivel técnico como operativo, debido a que esta plataforma puede estar vinculada con procesos de transferencia automatizada de archivos sensibles, tales como facturación, RIPS, autorizaciones, soportes médicos, resultados de laboratorio, información contractual e intercambio de datos con terceros. Entre las principales consecuencias se destacan las siguientes:

1. **Acceso no autorizado a plataformas de transferencia de archivos:**

   Los atacantes que exploten esta vulnerabilidad podrían evadir los mecanismos de autenticación y acceder sin autorización a la plataforma MOVEit Automation. Esto les permitiría consultar, descargar o interactuar con archivos transferidos entre sistemas internos, proveedores, aseguradores, IPS, EPS, laboratorios, operadores tecnológicos u otros terceros vinculados a la prestación de servicios de salud.

2. **Exposición de información sensible del sector salud:**

   Una explotación exitosa podría comprometer información clínica, administrativa, financiera o contractual. En el contexto sanitario, esto puede incluir datos personales de pacientes, historias clínicas, resultados diagnósticos, soportes de atención, órdenes médicas, autorizaciones, cuentas médicas, información de facturación, reportes RIPS y documentos asociados a la prestación de servicios de salud. La exposición de esta información representa un riesgo alto, al tratarse de datos personales sensibles protegidos por la normativa colombiana.

3. **Manipulación, eliminación o alteración de archivos críticos:**

   El acceso indebido a la plataforma podría permitir que un atacante modifique, elimine, reemplace o altere archivos utilizados en procesos operativos. Esto podría afectar la integridad de documentos clínicos, soportes administrativos, archivos de facturación, reportes regulatorios, registros de atención o información intercambiada con terceros, generando errores en procesos misionales y posibles inconsistencias en la trazabilidad de la información.

4. **Interrupción de flujos operativos esenciales:**

   La vulnerabilidad podría impactar procesos automatizados de transferencia de archivos que soportan actividades críticas en entidades de salud. Entre estos flujos pueden encontrarse la facturación de servicios, el envío y recepción de RIPS, la gestión de autorizaciones, el intercambio de soportes médicos, la remisión de resultados de laboratorio, la interoperabilidad con proveedores tecnológicos y la comunicación documental con aseguradores o entidades territoriales. La interrupción de estos procesos podría afectar la continuidad administrativa, financiera y asistencial.

5. **Compromiso de la cadena de terceros y proveedores:**

   En muchas entidades de salud, las plataformas de transferencia de archivos no operan de forma aislada, sino conectadas con proveedores externos, operadores de tecnología, aliados contractuales, laboratorios, aseguradoras o plataformas en la nube. Por esta razón, un acceso no autorizado podría extender el riesgo hacia terceros o permitir que un atacante utilice la plataforma comprometida como punto de entrada para acceder a otros sistemas relacionados.

6. **Escalamiento de privilegios y ampliación del compromiso:**

   Si la entidad afectada también presenta una segunda vulnerabilidad asociada, configuraciones inseguras, credenciales expuestas o controles de acceso deficientes, el

atacante podría escalar privilegios dentro del entorno comprometido. Esto aumentaría la posibilidad de tomar control de tareas automatizadas, modificar configuraciones, crear usuarios no autorizados, acceder a rutas de transferencia adicionales o moverse lateralmente hacia otros sistemas internos.

7. **Riesgo de pérdida de confidencialidad, integridad y disponibilidad:**

   La explotación de esta vulnerabilidad puede afectar los tres pilares de la seguridad de la información. La confidencialidad se vería comprometida por el acceso indebido a datos sensibles; la integridad, por la posibilidad de modificar o alterar archivos; y la disponibilidad, por la interrupción de flujos automatizados o la eliminación de información necesaria para la operación diaria de la entidad.

8. **Impacto reputacional e institucional:**

   La exposición de información clínica o administrativa puede generar pérdida de confianza por parte de pacientes, usuarios, proveedores, entes de control y aliados estratégicos. En el sector salud, este impacto reputacional puede ser especialmente crítico, ya que la protección de la información del paciente está directamente relacionada con la confianza en la prestación del servicio y con la responsabilidad institucional frente al manejo de datos sensibles.

9. **Riesgo regulatorio y legal:**

   Las entidades que traten datos personales o datos sensibles de salud podrían enfrentar investigaciones, requerimientos o sanciones por incumplimiento de obligaciones relacionadas con la protección de datos personales, seguridad de la información, reserva de la historia clínica y gestión adecuada de incidentes. En Colombia, este riesgo se relaciona especialmente con la Ley 1581 de 2012, las normas sobre tratamiento de datos sensibles y las obligaciones aplicables a los actores del sistema de salud.

10. **Mayor exposición en el contexto colombiano de ciberamenazas:**

    El riesgo adquiere mayor relevancia debido al panorama actual de amenazas en Colombia. MinTIC informó que durante 2024 el país enfrentó cerca de 36.000 millones de intentos de afectación, ubicándose como el segundo país más atacado de Latinoamérica, con especial impacto en los sectores financiero, salud y energético. Esto evidencia que las entidades de salud son objetivos relevantes para actores maliciosos y que vulnerabilidades críticas en plataformas de transferencia de archivos deben ser tratadas con prioridad alta.

Modo de explotación del ataque

La vulnerabilidad **CVE-2026-4670** puede ser explotada de forma remota, con baja complejidad, sin privilegios previos y sin interacción del usuario, de acuerdo con el vector CVSS publicado por NVD: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H. En términos prácticos, esto significa que un atacante que pueda alcanzar una instancia vulnerable de MOVEit Automation podría intentar omitir el proceso normal de autenticación y obtener acceso no autorizado a una plataforma utilizada para la transferencia automatizada de archivos empresariales.

El ataque podría iniciar con una fase de reconocimiento, en la cual el actor malicioso identifica instancias expuestas de **MOVEit Automation**, versiones vulnerables, interfaces accesibles, servicios asociados o configuraciones visibles desde internet o redes no confiables. Posteriormente, el atacante podría intentar explotar la debilidad de autenticación para evadir los controles de acceso y obtener entrada inicial a la plataforma.

Una vez dentro, el atacante podría enumerar tareas automatizadas, rutas de transferencia, usuarios, conectores, archivos procesados, servidores de origen y destino, así como integraciones con terceros. En una entidad de salud, esta fase representa un riesgo elevado,

dado que dichos flujos pueden estar relacionados con facturación, RIPS, autorizaciones, soportes médicos, resultados de laboratorio, cuentas médicas, información contractual, datos administrativos y documentación clínica.

Después del acceso inicial, el atacante podría consultar, descargar, modificar, eliminar o alterar archivos utilizados en procesos críticos. También podría manipular tareas programadas, afectar la integridad de la información transferida o interrumpir flujos operativos esenciales. Si además se encuentra presente la vulnerabilidad **CVE-2026-5174** u otras debilidades de configuración, el atacante podría escalar privilegios y obtener mayor control sobre la plataforma, incluyendo funciones administrativas o configuraciones sensibles.

El riesgo no debe evaluarse únicamente desde la perspectiva de acceso a una aplicación, sino como un posible compromiso de una plataforma que centraliza transferencias de información entre sistemas internos, terceros, proveedores y aliados estratégicos. En consecuencia, la explotación podría facilitar exposición de datos sensibles, movimiento lateral, afectación de la continuidad operativa, pérdida de trazabilidad documental y posibles incidentes de confidencialidad, integridad y disponibilidad.

No se recomienda esperar señales públicas de explotación activa para actuar. Aunque Progress no ha indicado explotación en la naturaleza al momento de los reportes consultados, antecedentes recientes demuestran que las soluciones MFT han sido objetivos de alto valor para actores de ransomware y grupos de robo de información. En 2023, vulnerabilidades previas de MOVEit Transfer fueron explotadas por el grupo Clop en campañas masivas de exfiltración de datos, lo que refuerza la necesidad de aplicar los parches disponibles, revisar la exposición de las instancias y realizar análisis de registros en busca de actividad anómala

.

Alerta Vulnerabilidad
Vulnerabilidad en MOVEit Automation

CSIRTSALUD-AV-202600506-45 **TLP: CLEAR**

Vulnerabilidades asociadas

Las vulnerabilidades asociadas a esta alerta corresponden a fallas de seguridad identificadas en Progress MOVEit Automation, una solución de transferencia administrada de archivos utilizada para automatizar flujos de intercambio de información entre sistemas empresariales. De acuerdo con la información publicada por NVD y reportes especializados, las fallas pueden permitir bypass de autenticación y escalamiento de privilegios, lo que representa un riesgo crítico para organizaciones que procesan información sensible, especialmente en sectores como salud, financiero y servicios esenciales.

Recomendaciones de detección y mitigación

Los equipos de seguridad, infraestructura y desarrollo deben priorizar la actualización inmediata de todos los entornos afectados hacia la versión corregida del framework y del runtime correspondiente. Microsoft ya publicó .NET 10.0.7 y ASP.NET Core Runtime 10.0.7, por lo que se recomienda verificar servidores, contenedores, imágenes base, pipelines de despliegue y componentes de hospedaje para asegurar que no permanezcan instancias desactualizadas en producción, pruebas o contingencia.

Adicionalmente, se recomienda realizar un inventario técnico de todas las aplicaciones que utilicen autenticación basada en cookies y mecanismos de ASP.NET Core Data Protection, dado que este subsistema es el encargado de proteger y validar información sensible como cookies y otros datos confiables enviados al cliente. Este ejercicio debe incluir la identificación del repositorio del key ring, el esquema de despliegue en múltiples nodos y las cuentas de servicio con acceso a dicho repositorio.

Alerta Vulnerabilidad
Vulnerabilidad en MOVEit Automation

CSIRTSALUD-AV-202600506-45 **TLP: CLEAR**

Tabla de vulnerabilidades identificadas

CVE	Producto afectado	Severidad	Descripción	Estado
CVE-2026-4670	MOVEit Automation	**Crítica — 9.8**	Vulnerabilidad de bypass de autenticación por debilidad primaria. Puede permitir que un atacante omita controles normales de autenticación y acceda a la plataforma sin credenciales válidas.	**Parche disponible**
CVE-2026-5174	MOVEit Automation	**Alta — 7.7**	Vulnerabilidad de validación incorrecta de entrada que podría permitir escalamiento de privilegios dentro de la plataforma afectada.	**Parche disponible**

1. CVE-2026-4670 — Bypass de autenticación

La vulnerabilidad CVE-2026-4670 corresponde a una falla crítica de bypass de autenticación en Progress MOVEit Automation. NVD la clasifica con un puntaje CVSS 3.1 de 9.8, bajo el vector AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, lo que indica que puede ser explotada de forma remota, con baja complejidad, sin privilegios previos y sin interacción del usuario.

Esta vulnerabilidad se encuentra asociada a CWE-305: Authentication Bypass by Primary Weakness, lo que significa que el problema está relacionado con una debilidad primaria en el mecanismo de autenticación. En términos prácticos, un atacante que logre alcanzar una instancia vulnerable podría intentar omitir el proceso normal de inicio de sesión y acceder a funcionalidades o recursos que deberían estar protegidos.

En una entidad de salud, esta vulnerabilidad es especialmente delicada porque MOVEit Automation puede estar vinculado con flujos de transferencia de archivos que contienen RIPS, facturación, autorizaciones, soportes médicos, resultados de laboratorio, cuentas médicas,

información contractual o documentos administrativos con datos personales y datos sensibles de salud.

2. CVE-2026-5174 — Validación incorrecta de entrada y posible escalamiento de privilegios

La vulnerabilidad CVE-2026-5174 fue reportada como una falla de severidad alta en MOVEit Automation, asociada a validación incorrecta de entrada y posible escalamiento de privilegios. The Hacker News reportó que esta vulnerabilidad tiene un puntaje CVSS de 7.7 y que, junto con CVE-2026-4670, puede permitir bypass de autenticación y escalamiento de privilegios a través de interfaces del puerto de comandos del backend del servicio.

El riesgo principal de esta segunda vulnerabilidad es que, si un atacante ya logró acceso inicial o si existe una configuración insegura en el entorno, podría ampliar sus permisos dentro de la plataforma. Esto podría permitirle obtener control administrativo, modificar configuraciones, alterar tareas automatizadas, acceder a rutas adicionales de transferencia o manipular archivos procesados por el sistema.

En el contexto de una entidad de salud, el escalamiento de privilegios podría agravar significativamente el incidente, ya que permitiría pasar de un acceso no autorizado inicial a un nivel de control superior sobre procesos críticos de intercambio de información.

Versiones afectadas reportadas

Las versiones afectadas corresponden a ramas vulnerables de MOVEit Automation que deben ser actualizadas a las versiones corregidas publicadas por el fabricante. The Hacker News reportó las siguientes ramas y versiones corregidas:

Rama de MOVEit Automation	Versión vulnerable	Versión corregida
2025.1.x	≤ 2025.1.4	2025.1.5

Rama de MOVEit Automation	Versión vulnerable	Versión corregida
2025.0.x	≤ 2025.0.8	2025.0.9
2024.1.x	≤ 2024.1.7	2024.1.8

Adicionalmente, NVD indica que CVE-2026-4670 afecta versiones desde 2025.0.0 antes de 2025.0.9, desde 2024.0.0 antes de 2024.1.8 y versiones anteriores a 2024.0.0. Por criterio preventivo, cualquier instalación antigua, no soportada o por debajo de las versiones corregidas debe considerarse de alto riesgo hasta que sea validada y actualizada.

Recomendaciones de detección y mitigación

Teniendo en cuenta que la vulnerabilidad CVE-2026-4670 permite bypass de autenticación en Progress MOVEit Automation y que puede ser explotada de forma remota, con baja complejidad, sin privilegios previos y sin interacción del usuario, las organizaciones del sector salud deben adoptar medidas inmediatas de validación, detección, contención y mitigación. La NVD registra esta vulnerabilidad con vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H y puntaje 9.8 crítico, lo que justifica su tratamiento como una prioridad alta de seguridad.

Las medidas recomendadas deben ser ejecutadas de forma coordinada entre las áreas de tecnología, seguridad de la información, infraestructura, gestión de proveedores, continuidad del negocio y protección de datos personales, especialmente cuando la plataforma esté involucrada en procesos de intercambio de información clínica, financiera, administrativa o contractual.

- **Validación inicial**

Como primera medida, las entidades deben realizar una validación inmediata para determinar si existe exposición directa o indirecta a la vulnerabilidad. Esta revisión no debe limitarse únicamente a los activos administrados internamente, ya que MOVEit Automation puede estar

operando a través de terceros, proveedores tecnológicos, operadores de servicios administrados o aliados que procesan información de la organización.

Las áreas de tecnología, seguridad de la información y proveedores deben verificar:

Uso directo de MOVEit Automation:

Confirmar si la organización tiene instalada, contratada o administrada alguna instancia de MOVEit Automation en ambientes productivos, de pruebas, contingencia, respaldo o desarrollo.

Uso indirecto a través de terceros:

Validar si algún proveedor crítico, operador tecnológico, integrador, laboratorio, plataforma de facturación, gestor documental, aliado contractual o tercero encargado del tratamiento de información utiliza MOVEit Automation para procesar, almacenar o transferir archivos de la entidad.

Exposición a internet:

Identificar si existen instancias de MOVEit Automation accesibles desde internet, redes públicas, canales externos, conexiones remotas o segmentos de red no controlados. Las instancias expuestas públicamente deben considerarse de riesgo elevado hasta que se confirme su versión y estado de actualización.

Versión instalada:

Determinar la versión exacta instalada de MOVEit Automation. Las versiones afectadas incluyen ramas anteriores a **2025.1.5**, **2025.0.9** y **2024.1.8**, de acuerdo con los reportes publicados sobre las versiones corregidas.

Integraciones críticas:

Revisar si la plataforma tiene integraciones con sistemas clínicos, financieros, RIPS, facturación, autorizaciones, laboratorios, repositorios documentales, sistemas de gestión hospitalaria, plataformas de interoperabilidad, almacenamiento en nube o servicios de terceros.

Tipo de información transferida:

Identificar qué clases de archivos circulan por la plataforma, especialmente si contienen datos personales, datos sensibles de salud, historias clínicas, resultados diagnósticos, cuentas médicas, soportes de atención, información contractual o documentos financieros.

Responsables técnicos y contractuales:

Definir responsables internos y externos para la validación, actualización, revisión de registros y documentación de evidencias. En caso de uso tercerizado, se debe solicitar al proveedor confirmación formal del estado de actualización y de las acciones de revisión aplicadas.

- **Revisión técnica**

Una vez confirmada la existencia de MOVEit Automation en la organización o en un tercero crítico, se recomienda realizar una revisión técnica detallada para identificar posibles señales de acceso indebido, manipulación de configuraciones o uso anómalo de la plataforma.

Se recomienda revisar, como mínimo, los siguientes elementos:

Logs de autenticación:

Analizar inicios de sesión exitosos y fallidos, accesos desde ubicaciones inusuales, sesiones fuera del comportamiento normal, autenticaciones sin trazabilidad esperada, accesos con cuentas privilegiadas y eventos asociados a usuarios desconocidos o inactivos.

Logs administrativos:

Revisar cambios en configuración, modificación de parámetros del sistema, ajustes en políticas de transferencia, cambios en rutas, alteración de tareas automatizadas, creación de conectores o modificación de servicios vinculados.

Transferencias recientes:

Validar transferencias ejecutadas en los últimos días o semanas, especialmente aquellas que involucren grandes volúmenes de información, destinos no habituales, horarios atípicos, archivos comprimidos, nombres de archivo inusuales o conexiones hacia terceros no reconocidos.

Cambios en tareas automatizadas:

Revisar si se crearon, modificaron, deshabilitaron o eliminaron tareas programadas sin autorización. En plataformas MFT, la manipulación de tareas puede permitir redireccionar archivos, duplicar transferencias o alterar flujos operativos críticos.

Creación o modificación de usuarios:

Verificar la aparición de cuentas nuevas, cambios en cuentas existentes, activación de usuarios deshabilitados, modificación de roles, cambios de contraseña, asignación de privilegios administrativos o creación de cuentas de servicio no documentadas.

Cambios de permisos:

Analizar modificaciones en perfiles, roles, privilegios, permisos sobre carpetas, permisos sobre rutas de transferencia, acceso a conectores y autorización para ejecutar tareas o administrar la plataforma.

Conexiones desde direcciones IP no reconocidas:

Identificar accesos provenientes de direcciones IP externas, países no esperados, proveedores de hosting, redes anónimas, VPN desconocidas, direcciones no asociadas a la operación normal o conexiones repetitivas desde orígenes sospechosos.

Fallos repetitivos de autenticación:

Revisar patrones de múltiples intentos fallidos, errores repetidos sobre cuentas administrativas, intentos sobre usuarios inexistentes o comportamiento compatible con enumeración de usuarios o pruebas automatizadas.

Actividad fuera de horarios operativos:

Verificar accesos, transferencias, cambios de configuración o ejecución de tareas en horarios no habituales, fines de semana, festivos o ventanas en las que normalmente no se ejecutan procesos administrativos.

Actividad en interfaces del backend o puertos de comando:

Considerando que los reportes señalan que estas vulnerabilidades pueden involucrar interfaces del puerto de comandos del backend del servicio, se recomienda revisar cualquier actividad anómala asociada a dichos componentes, especialmente si proviene de redes no autorizadas.

Integridad de archivos procesados:

Comparar archivos recientes contra registros esperados, hash de integridad, controles de recepción, trazabilidad documental o confirmaciones de terceros, especialmente en flujos relacionados con RIPS, facturación, autorizaciones, resultados de laboratorio y soportes médicos.

Eventos correlacionados en otras plataformas:

Revisar registros en firewalls, WAF, SIEM, EDR, servidores de archivos, bases de datos, sistemas clínicos, sistemas financieros, repositorios documentales y plataformas de almacenamiento en nube para identificar actividad relacionada con la posible explotación.

- **Mitigación prioritaria**

La medida principal de mitigación es actualizar inmediatamente MOVEit Automation a la versión corregida correspondiente. The Hacker News reportó que no existen soluciones alternativas que resuelvan completamente estas vulnerabilidades, por lo que la aplicación de las versiones corregidas debe ser tratada como acción prioritaria

Se recomienda aplicar las siguientes medidas:

1. **Actualizar inmediatamente la plataforma:**

   Instalar la versión corregida correspondiente según la rama utilizada:

Rama de MOVEit Automation	Versión vulnerable	Versión corregida
2025.1.x	≤ 2025.1.4	2025.1.5
2025.0.x	≤ 2025.0.8	2025.0.9
2024.1.x	≤ 2024.1.7	2024.1.8

2. **Restringir la exposición pública:**
   Limitar cualquier acceso directo desde internet a la plataforma. Si la exposición pública no es estrictamente necesaria, debe deshabilitarse. Si es requerida por operación, debe quedar protegida mediante controles robustos de red, autenticación, monitoreo y segmentación.
3. **Limitar el acceso mediante VPN, ACL o segmentación de red:**
   Permitir acceso únicamente desde redes, direcciones IP, segmentos o usuarios autorizados. Se

recomienda aplicar listas de control de acceso, reglas específicas en firewall, segmentación de red y acceso mediante VPN corporativa.

4. **Rotar credenciales asociadas a flujos automatizados:**
   Cambiar contraseñas, tokens, credenciales de integración, credenciales de cuentas de servicio y credenciales usadas en conectores. Esta medida es especialmente importante si la plataforma pudo haber estado expuesta antes de aplicar el parche.
5. **Revisar llaves API, secretos, cuentas de servicio y certificados:**
   Validar si existen llaves API, secretos, certificados digitales, claves privadas o tokens almacenados o referenciados dentro de la plataforma. Los elementos sensibles deben rotarse si existe sospecha de exposición.
6. **Aplicar principio de privilegio mínimo:**
   Verificar que las cuentas de servicio y usuarios administrativos tengan únicamente los permisos necesarios. Se deben eliminar privilegios excesivos, cuentas obsoletas, usuarios genéricos y accesos que no estén justificados por una necesidad operativa.
7. **Revisar y depurar cuentas administrativas:**
   Confirmar que todas las cuentas con privilegios elevados correspondan a usuarios autorizados, activos y plenamente identificados. Se recomienda eliminar cuentas compartidas y exigir autenticación fuerte cuando esté disponible.
8. **Validar integraciones con terceros:**
   Solicitar a proveedores críticos evidencia de actualización, revisión de logs y controles aplicados. Esta validación debe quedar documentada, especialmente cuando el tercero procese datos personales, información clínica, facturación, RIPS o soportes médicos de la entidad.
9. **Activar monitoreo reforzado durante al menos 30 días:**
   Establecer monitoreo intensivo sobre autenticación, transferencias, cambios administrativos, tareas automatizadas, conexiones externas, creación de usuarios, modificación de permisos y actividad fuera de horario. El periodo mínimo recomendado es de **30 días**, aunque puede ampliarse si se identifican señales sospechosas.

10. **Correlacionar eventos en SIEM o herramientas de monitoreo:**
    Integrar logs de MOVEit Automation con SIEM, EDR, firewalls, WAF, plataformas de monitoreo y herramientas de respuesta a incidentes. La correlación permite detectar patrones que podrían pasar desapercibidos si se revisa cada fuente de forma aislada.
11. **Respaldar configuración y evidencias antes de cambios críticos:**
    Antes de realizar actualizaciones o intervenciones mayores, se recomienda preservar respaldos, configuraciones actuales, logs relevantes y evidencias técnicas. Esto permite análisis posterior en caso de que se confirme un incidente.
12. **Documentar la gestión de la vulnerabilidad:**
    Registrar fecha de identificación, versión instalada, responsable de validación, evidencia de actualización, resultados de revisión de logs, proveedores consultados, medidas aplicadas y decisiones tomadas. Esta documentación es clave para auditoría, trazabilidad y cumplimiento normativo

- **Medidas específicas para entidades del sector salud**

Dado que las organizaciones del sector salud procesan información especialmente sensible, se recomienda complementar la mitigación técnica con acciones orientadas a continuidad operativa, protección de datos personales y gestión de terceros.

1. **Priorizar flujos críticos de salud:**
   Revisar con prioridad los flujos relacionados con RIPS, facturación, autorizaciones, resultados de laboratorio, historias clínicas, soportes médicos, cuentas médicas y reportes administrativos.
2. **Validar impacto sobre datos personales sensibles:**
   Determinar si por MOVEit Automation circulan datos de pacientes, diagnósticos, procedimientos, resultados, información financiera o documentos clínicos. Si existe sospecha de exposición, debe activarse el procedimiento interno de gestión de incidentes de seguridad de la información.

3. **Revisar continuidad de procesos operativos:**
   Confirmar que la actualización o restricción de accesos no interrumpa procesos críticos. En caso de requerirse ventanas de mantenimiento, deben coordinarse con las áreas asistenciales, administrativas y financieras.
4. **Involucrar al oficial de protección de datos o responsable equivalente:**
   Cuando exista posible exposición de información personal o sensible, debe participar el responsable de protección de datos personales, jurídico, cumplimiento y seguridad de la información.
5. **Exigir certificación o constancia a proveedores:**
   Cuando MOVEit Automation sea operado por terceros, se recomienda solicitar constancia formal de actualización, versión corregida aplicada, fecha de mitigación y revisión de actividad sospechosa
6.

Recomendaciones de prevención y mitigación

1. Como medida de prevención y mitigación, las organizaciones del sector salud deben actualizar inmediatamente Progress MOVEit Automation a la versión corregida correspondiente, de acuerdo con la rama instalada: 2025.1.5, 2025.0.9 o 2024.1.8. Esta acción debe ser prioritaria, ya que la vulnerabilidad CVE-2026-4670 permite bypass de autenticación y fue clasificada con severidad crítica. Adicionalmente, la vulnerabilidad asociada CVE-2026-5174 puede permitir escalamiento de privilegios, lo que incrementa el riesgo de control administrativo y exposición de datos.
2. Las entidades no deben depender únicamente de medidas compensatorias, debido a que los reportes disponibles indican que no existen soluciones alternativas que corrijan completamente el problema. Por tanto, la actualización debe complementarse con restricción de exposición pública, segmentación de red, acceso mediante VPN, listas de

control de acceso, autenticación multifactor, rotación de credenciales, revisión de llaves API, secretos, cuentas de servicio y certificados.

3. También se recomienda fortalecer los controles sobre los flujos críticos del sector salud, especialmente aquellos relacionados con RIPS, facturación, autorizaciones, soportes médicos, resultados de laboratorio, historias clínicas, cuentas médicas, información contractual y repositorios documentales. Estos flujos deben contar con controles de confidencialidad, integridad, trazabilidad, cifrado y monitoreo continuo.
4. En relación con terceros, las entidades deben confirmar si proveedores críticos utilizan MOVEit Automation para procesar información institucional. En caso afirmativo, se debe solicitar evidencia formal de actualización, revisión de registros, restricción de accesos, rotación de credenciales y aplicación de controles de seguridad. Esta validación debe quedar documentada para fines de auditoría, cumplimiento y gestión de riesgos.
5. Finalmente, se recomienda mantener monitoreo reforzado durante al menos 30 días posteriores a la actualización, revisar eventos administrativos, transferencias inusuales, conexiones no reconocidas y cambios de configuración, así como actualizar los planes de respaldo, continuidad y respuesta a incidentes. Estas medidas permiten reducir la probabilidad de explotación, limitar el impacto ante un posible compromiso y fortalecer la resiliencia de las plataformas que soportan el intercambio de información sensible en el sector salud.

Recomendaciones de respuesta ante compromiso

En caso de que la entidad identifique indicios de explotación, acceso no autorizado, transferencias anómalas, modificación de tareas automatizadas, creación de usuarios no reconocidos o posible exposición de información sensible mediante **Progress MOVEit**

Automation, se debe activar de manera inmediata el procedimiento interno de respuesta a incidentes de seguridad de la información.

La respuesta debe tratarse con prioridad alta, considerando que la vulnerabilidad CVE-2026-4670 permite bypass de autenticación y tiene severidad crítica CVSS 9.8, mientras que la vulnerabilidad asociada CVE-2026-5174 puede permitir escalamiento de privilegios. Progress indicó que estas fallas pueden derivar en acceso no autorizado, control administrativo y exposición de datos, y que la actualización mediante instalador completo es la única forma de remediar el problema.

Activación del procedimiento de respuesta a incidentes

La entidad debe activar formalmente su procedimiento de gestión de incidentes, involucrando como mínimo a las áreas de:

- Seguridad de la información.
- Infraestructura y tecnología.
- Continuidad del negocio.
- Protección de datos personales.
- Jurídica y cumplimiento.
- Gestión de proveedores.

Líderes de procesos afectados, especialmente si existen flujos relacionados con RIPS, facturación, autorizaciones, laboratorios, soportes médicos o repositorios documentales.

El incidente debe clasificarse según su criticidad, alcance preliminar, tipo de información comprometida, sistemas afectados y posible impacto sobre datos personales o datos sensibles de salud.

Contención inicial

La primera acción debe orientarse a limitar la capacidad del atacante para mantener acceso, extraer información o manipular archivos.

Se recomienda:

- **Aislar temporalmente la instancia afectada**, cuando sea viable operativamente, especialmente si se encuentra expuesta a internet.
- **Restringir accesos externos** mediante firewall, listas de control de acceso, VPN o segmentación de red.
- **Bloquear direcciones IP sospechosas** identificadas en logs, firewalls, SIEM, WAF u otras herramientas de monitoreo.
- **Suspender cuentas sospechosas o no reconocidas**, especialmente cuentas administrativas, cuentas de servicio o usuarios creados recientemente.
- **Deshabilitar tareas automatizadas no validadas**, principalmente aquellas que transfieran información sensible hacia destinos externos.
- **Evitar apagar o reinstalar el sistema de forma inmediata** sin preservar evidencias, salvo que exista riesgo activo de exfiltración, destrucción de información o afectación grave de la operación.

La contención debe equilibrar dos objetivos: detener el posible compromiso y conservar suficiente evidencia para determinar qué ocurrió, cuándo ocurrió, qué información pudo verse afectada y qué usuarios o sistemas estuvieron involucrados.

Preservación de evidencias

Antes de realizar cambios mayores sobre la plataforma, se deben preservar evidencias técnicas que permitan adelantar análisis forense, trazabilidad interna, soporte regulatorio y documentación del incidente.

Se recomienda conservar:

- Logs de autenticación.
- Logs administrativos.
- Historial de transferencias.
- Registros de creación, modificación o eliminación de usuarios.
- Cambios de permisos y roles.
- Cambios en tareas automatizadas.
- Configuración actual de la plataforma.
- Registros de firewall, WAF, VPN, SIEM, EDR y servidores relacionados.
- Direcciones IP de origen y destino.
- Listado de archivos transferidos, consultados, modificados o eliminados.
- Evidencia de versiones instaladas y fecha de aplicación de parches.

Estas evidencias deben conservarse con cadena de custodia interna, indicando fecha, hora, responsable, fuente del registro y método de extracción. En caso de posible exposición de datos personales, esta documentación será clave para soportar las decisiones ante autoridades, titulares de datos, auditorías internas o investigaciones posteriores.

Análisis de alcance e impacto

Una vez contenida la amenaza inicial, la entidad debe determinar el alcance real o probable del compromiso.

Se recomienda validar:

- Fecha probable de inicio del compromiso.
- Usuarios o cuentas utilizadas durante el acceso no autorizado.

- Direcciones IP involucradas.
- Tareas automatizadas ejecutadas durante el periodo sospechoso.
- Archivos transferidos, descargados, modificados o eliminados.
- Sistemas internos o terceros conectados a MOVEit Automation.
- Tipo de información afectada.
- Volumen aproximado de registros comprometidos.
- Posible afectación de datos personales o datos sensibles de salud.
- Impacto sobre continuidad operativa, facturación, RIPS, autorizaciones, resultados de laboratorio o soportes médicos.

En el sector salud, se debe prestar especial atención a información relacionada con historias clínicas, diagnósticos, procedimientos, resultados de laboratorio, órdenes médicas, autorizaciones, cuentas médicas, datos de identificación de pacientes e información financiera asociada a la prestación del servicio. La Ley 1581 de 2012 aplica al tratamiento de datos personales en Colombia, y la Ley 2015 de 2020 exige condiciones de privacidad y reserva en el marco de la interoperabilidad de la historia clínica electrónica.

Erradicación de la amenaza

Después de identificar el alcance preliminar, la entidad debe eliminar los mecanismos que pudieron permitir el acceso indebido o la persistencia del atacante.

Se recomienda:

- Actualizar MOVEit Automation a la versión corregida correspondiente:
- 2025.1.x → 2025.1.5
- 2025.0.x → 2025.0.9
- 2024.1.x → 2024.1.8

- Eliminar cuentas no autorizadas o sospechosas.
- Restablecer permisos modificados indebidamente.
- Revertir cambios no autorizados en tareas automatizadas.
- Eliminar conectores, rutas o destinos de transferencia no reconocidos.
- Rotar credenciales asociadas a flujos automatizados.
- Rotar llaves API, secretos, certificados y tokens utilizados por la plataforma.
- Revisar cuentas de servicio con privilegios excesivos.
- Validar que no existan mecanismos de persistencia en servidores relacionados.
- Correlacionar eventos con EDR, SIEM, firewall, WAF, VPN y servidores de archivos.

La erradicación no debe limitarse a instalar el parche. Si existió acceso no autorizado antes de la actualización, se debe asumir que credenciales, rutas, secretos, configuraciones o información transferida pudieron haber sido observados o manipulados.

Recuperación segura de la operación

La plataforma solo debe volver a operación normal cuando existan condiciones mínimas de seguridad verificadas.

Antes de restablecer servicios, se recomienda confirmar:

- Versión corregida instalada.
- Controles de acceso revisados.
- Cuentas sospechosas eliminadas o bloqueadas.
- Credenciales críticas rotadas.
- Tareas automatizadas verificadas.

- Rutas de transferencia validadas.
- Integridad de archivos críticos confirmada.
- Exposición pública restringida.
- Monitoreo reforzado activo.
- Plan de contingencia disponible en caso de recurrencia.

En procesos de salud, la recuperación debe priorizar flujos críticos como RIPS, facturación, autorizaciones, resultados de laboratorio, soportes médicos, cuentas médicas y comunicaciones con terceros esenciales, evitando reactivar transferencias sin validar previamente su legitimidad e integridad.

Notificación y gestión regulatoria

Si el análisis confirma o sugiere posible exposición, pérdida, alteración, acceso no autorizado o uso indebido de datos personales, la entidad debe evaluar sus obligaciones de reporte conforme al régimen colombiano de protección de datos personales.

La Superintendencia de Industria y Comercio ha señalado que, cuando el responsable del tratamiento esté obligado a reportar sus bases de datos, los incidentes de seguridad deben reportarse a través del Registro Nacional de Bases de Datos dentro de los quince días hábiles siguientes al momento en que sean detectados y puestos en conocimiento del área encargada.

Adicionalmente, la SIC cuenta con una guía para la gestión de incidentes de seguridad en el tratamiento de datos personales, orientada a responsables y encargados del tratamiento para manejar incidentes que puedan afectar información personal bajo su custodia.

Se recomienda:

- Evaluar si el incidente involucra datos personales o datos sensibles de salud.
- Determinar si procede reporte ante la SIC.

- Documentar la fecha de detección y la fecha de conocimiento por el área responsable.
- Preparar descripción del incidente, sistemas afectados, tipo de datos involucrados y medidas adoptadas.
- Evaluar si corresponde informar a titulares de datos afectados.
- Coordinar con jurídica, protección de datos y alta dirección antes de comunicaciones externas.
- Evaluar comunicaciones contractuales con EPS, IPS, E.S.E., laboratorios, operadores tecnológicos o proveedores involucrados.
- Registrar todas las decisiones tomadas durante la gestión del incidente.

Comunicación interna y externa

La comunicación debe ser controlada, verificable y coordinada. No se recomienda emitir comunicaciones públicas o a terceros sin contar con una evaluación técnica mínima del alcance del incidente.

Se recomienda:

- Definir voceros autorizados.
- Evitar especulaciones sobre datos comprometidos antes del análisis técnico.
- Informar internamente a las áreas afectadas sobre medidas temporales.
- Notificar a terceros críticos si sus integraciones pudieron verse afectadas.
- Preparar mensajes para usuarios, pacientes o titulares solo si el análisis determina posible afectación.
- Conservar evidencia de las comunicaciones realizadas.

La comunicación debe ser clara, proporcional y basada en hechos confirmados: qué ocurrió, qué sistemas estuvieron involucrados, qué información pudo estar afectada, qué medidas se tomaron y cuáles son los pasos siguientes.

Monitoreo posterior al incidente

Después de la contención, actualización y recuperación, se debe mantener monitoreo reforzado durante al menos 30 días, o por más tiempo si el análisis evidencia exposición prolongada o actividad sospechosa.

Se recomienda monitorear:

- Intentos de acceso no autorizado.
- Uso de cuentas administrativas.
- Transferencias inusuales o de alto volumen.
- Conexiones desde IP no reconocidas.
- Creación o modificación de usuarios.
- Cambios en tareas automatizadas.
- Cambios de permisos.
- Actividad fuera de horarios operativos.
- Conexiones hacia destinos externos no habituales.
- Alertas en EDR, SIEM, WAF, firewall y sistemas relacionados.

El monitoreo posterior debe buscar tanto señales de explotación de la vulnerabilidad como indicios de persistencia, movimiento lateral, reutilización de credenciales o intentos de exfiltración.

Alerta Vulnerabilidad
Vulnerabilidad en MOVEit Automation

CSIRTSALUD-AV-202600506-45 **TLP: CLEAR**

Conclusiones

La vulnerabilidad CVE-2026-4670 en MOVEit Automation representa un riesgo alto para entidades de salud que usen esta plataforma o dependan de proveedores que la utilicen. El principal riesgo es el acceso no autorizado a sistemas de transferencia de archivos, lo que puede derivar en exposición de datos sensibles, afectación operativa y compromiso de procesos misionales.

Aunque no hay confirmación pública de explotación activa contra organizaciones de salud en Colombia, el contexto nacional exige atención prioritaria, dado que el sector salud es uno de los sectores más expuestos a ciberamenazas en el país.

Acción concreta recomendada: validar exposición, aplicar parches, solicitar confirmación formal a proveedores y revisar logs de los últimos 30 días.

Fuentes:

- NVD — CVE-2026-4670: descripción, severidad, vector CVSS y versiones afectadas. https://nvd.nist.gov/vuln/detail/CVE-2026-4670
- BleepingComputer — Progress advierte falla crítica de bypass de autenticación en MOVEit Automation. https://www.bleepingcomputer.com/news/security/moveit-automation-customers-warned-to-patch-critical-auth-bypass-flaw/
- The Hacker News — Progress corrige fallas críticas y altas en MOVEit Automation. https://thehackernews.com/2026/05/progress-patches-critical-moveit.html
- MinTIC — Estrategia Nacional de Seguridad Digital y contexto de ciberamenazas en Colombia https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/403023:La-

Estrategia-Nacional-de-Seguridad-Digital-llega-para-enfrentar-las-crecientes-amenazas-ciberneticas

-

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.