

Alerta ID:	54
Fecha del reporte:	15/07/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades críticas activamente explotadas en Microsoft SharePoint permiten ejecución remota de código (RCE).
Herramienta de detección	N/A
Activo involucrado:	Servidores Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019 y Microsoft SharePoint Server 2016 implementados en entornos locales (On-Premises); servidores Microsoft Internet Information Services (IIS) que hospedan plataformas SharePoint; servidores Microsoft Windows que soportan la infraestructura de colaboración; bases de datos Microsoft SQL Server asociadas a las granjas SharePoint; servicios de Active Directory y Microsoft Entra ID integrados para procesos de autenticación e identidad; plataformas de gestión documental (ECM), portales institucionales, intranets corporativas y repositorios documentales; bibliotecas de documentos, listas, sitios de colaboración y aplicaciones empresariales integradas con SharePoint; sistemas de Historia Clínica Electrónica (HCE), plataformas de gestión administrativa, sistemas de interoperabilidad, aplicaciones de gestión hospitalaria y demás soluciones que almacenen, procesen o compartan información institucional mediante Microsoft SharePoint. También se consideran involucrados los servidores de aplicaciones, componentes de búsqueda, servicios distribuidos, servidores web front-end (WFE), servidores de aplicaciones SharePoint, servidores de indexación, servidores de autenticación, infraestructura de virtualización, dispositivos de seguridad perimetral y cualquier otro activo tecnológico que interactúe directa o indirectamente con la plataforma SharePoint dentro de organizaciones del sector salud.
Tipo de alerta:	Alerta
Nivel de riesgo:	Crítico

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre las vulnerabilidades críticas que afectan a Microsoft SharePoint Server y que están siendo explotadas activamente por actores de amenaza para obtener ejecución remota de código (Remote Code Execution – RCE), comprometer servidores expuestos a Internet, instalar componentes maliciosos, acceder de manera no autorizada a información institucional y utilizar los sistemas comprometidos como punto de entrada hacia otros activos tecnológicos de la organización.

Estas vulnerabilidades afectan plataformas Microsoft SharePoint implementadas en entornos locales (On-Premises) y representan un riesgo significativo para las entidades que utilizan esta tecnología como plataforma de colaboración, gestión documental, publicación de información institucional, intercambio de documentos, automatización de procesos o integración con aplicaciones críticas del negocio. La explotación exitosa puede comprometer la confidencialidad, integridad y disponibilidad de la información almacenada en SharePoint, además de facilitar el movimiento lateral hacia otros sistemas corporativos, el robo de credenciales, la instalación de web shells y la persistencia dentro de la infraestructura tecnológica.

Las organizaciones del sector salud presentan un nivel de exposición particularmente elevado debido a que numerosas instituciones utilizan Microsoft SharePoint para soportar procesos administrativos, documentales y asistenciales, incluyendo la gestión de procedimientos, protocolos clínicos, manuales institucionales, registros administrativos, documentación contractual, información de talento humano, proyectos de investigación, procesos de calidad, sistemas integrados de gestión y, en algunos casos, componentes asociados con plataformas de Historia Clínica Electrónica (HCE) o soluciones de interoperabilidad.

Adicionalmente, la Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA) ha emitido lineamientos específicos de endurecimiento (hardening) para Microsoft SharePoint con el propósito de reducir la superficie de ataque y fortalecer la protección de estas plataformas frente a campañas de explotación observadas recientemente. La adopción oportuna de estas recomendaciones, junto con la aplicación de las actualizaciones de seguridad publicadas por Microsoft, constituye una medida prioritaria para disminuir el riesgo de compromiso de los servidores afectados.

El propósito de esta alerta es proporcionar a las organizaciones del sector salud información técnica que facilite la identificación de activos potencialmente vulnerables, la evaluación de su nivel de exposición, la implementación de medidas preventivas y de endurecimiento, el fortalecimiento de los mecanismos de monitoreo y detección, y la preparación de procedimientos de respuesta que permitan contener oportunamente posibles intentos de explotación y preservar la continuidad de los servicios tecnológicos que soportan la atención en salud.

Descripción:

Las vulnerabilidades recientemente identificadas en Microsoft SharePoint Server representan una amenaza crítica para las organizaciones que utilizan esta plataforma como solución de colaboración, gestión documental y administración de contenidos empresariales. De acuerdo con la información publicada por Microsoft y la Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA), estas vulnerabilidades están siendo explotadas activamente por actores de amenaza para comprometer servidores SharePoint expuestos, ejecutar código arbitrario de forma remota y obtener acceso persistente a los entornos afectados. Este escenario incrementa significativamente el riesgo para organizaciones que administran información sensible o prestan servicios esenciales, como las entidades del sector salud.

Microsoft SharePoint es una plataforma ampliamente utilizada para la administración de documentos, automatización de procesos, publicación de portales corporativos y colaboración entre usuarios. Debido a su integración con servicios como Active Directory, Microsoft SQL Server, Microsoft Entra ID, Microsoft Office y otras aplicaciones empresariales, un compromiso exitoso del servidor puede proporcionar al atacante acceso privilegiado a recursos críticos de la organización, facilitando la expansión del incidente hacia otros sistemas de información.

Las campañas de explotación observadas demuestran que los actores de amenaza buscan comprometer servidores SharePoint accesibles desde Internet mediante el aprovechamiento de vulnerabilidades que permiten la ejecución remota de código (Remote Code Execution – RCE). Una vez obtenido el acceso inicial, los atacantes pueden desplegar web shells, ejecutar comandos arbitrarios, crear mecanismos de persistencia, instalar herramientas de administración remota, extraer credenciales, acceder a información almacenada en la

plataforma y utilizar el servidor comprometido como punto de apoyo para realizar movimientos laterales dentro de la infraestructura tecnológica institucional.

La instalación de una web shell constituye una de las principales actividades posteriores a la explotación. Este tipo de componente malicioso permite al atacante mantener acceso remoto al servidor mediante solicitudes HTTP o HTTPS aparentemente legítimas, ejecutar instrucciones directamente sobre el sistema operativo, cargar o descargar archivos, modificar el contenido de los sitios hospedados, crear nuevas cuentas de usuario y desplegar herramientas adicionales sin requerir nuevamente la explotación de la vulnerabilidad inicial. Esta capacidad dificulta la detección temprana del compromiso y favorece la permanencia del atacante dentro del entorno afectado.

Una vez comprometido el servidor SharePoint, el actor de amenaza puede desarrollar actividades de reconocimiento para identificar la arquitectura tecnológica de la organización, enumerar usuarios y grupos de Active Directory, identificar servidores conectados, localizar recursos compartidos, descubrir aplicaciones integradas y recopilar información sobre la infraestructura de autenticación. Esta información resulta fundamental para planificar fases posteriores del ataque, incluyendo el movimiento lateral hacia otros servidores, el compromiso de cuentas privilegiadas y la afectación de servicios críticos para la operación institucional.

En el sector salud, el impacto de estas vulnerabilidades adquiere una relevancia especial debido a que Microsoft SharePoint suele utilizarse como plataforma para la gestión documental institucional, administración de procedimientos asistenciales, almacenamiento de protocolos clínicos, publicación de manuales operativos, intercambio de documentación administrativa, gestión de proyectos, soporte a procesos de calidad y administración de información relacionada con la prestación de servicios de salud. En algunas organizaciones, la plataforma también se integra con sistemas de Historia Clínica Electrónica (HCE), soluciones de interoperabilidad y aplicaciones corporativas que procesan información sensible de pacientes.

La explotación exitosa de estas vulnerabilidades puede comprometer la confidencialidad de información clínica, administrativa, financiera y contractual, afectar la integridad de documentos institucionales, alterar procedimientos operativos, interrumpir procesos críticos de colaboración y generar indisponibilidad de servicios tecnológicos esenciales. Adicionalmente, el acceso obtenido sobre el servidor SharePoint puede facilitar la ejecución de ataques de

ransomware, campañas de espionaje, robo de información o actividades orientadas a la exfiltración de datos sensibles.

Uno de los aspectos que incrementa la criticidad de este escenario es la disponibilidad pública de técnicas de explotación y el interés demostrado por grupos de ciberdelincuencia y actores patrocinados por Estados en comprometer servidores SharePoint vulnerables. La rápida incorporación de estas técnicas en campañas automatizadas reduce el tiempo disponible para que las organizaciones implementen las actualizaciones de seguridad y las medidas de endurecimiento recomendadas, aumentando la probabilidad de compromiso de aquellos servidores que permanezcan expuestos y sin las correcciones correspondientes.

Ante este panorama, CISA recomienda a las organizaciones adoptar un enfoque de defensa en profundidad que combine la aplicación inmediata de las actualizaciones de seguridad publicadas por Microsoft con la implementación de medidas de hardening, el fortalecimiento de los mecanismos de autenticación, el monitoreo continuo de eventos de seguridad, la revisión de indicadores de compromiso y la validación periódica de la integridad de los servidores SharePoint. Estas acciones permiten reducir la superficie de ataque, mejorar la capacidad de detección temprana y fortalecer la respuesta frente a posibles intentos de explotación dirigidos contra la infraestructura tecnológica del sector salud.

Consecuencias de la explotación

La explotación exitosa de las vulnerabilidades que afectan a Microsoft SharePoint puede generar impactos significativos sobre la confidencialidad, integridad y disponibilidad de la información institucional, así como comprometer la infraestructura tecnológica que soporta los procesos misionales de las organizaciones del sector salud. Debido a que SharePoint suele integrarse con múltiples servicios corporativos y centraliza grandes volúmenes de información documental, un compromiso de esta plataforma puede trascender el servidor afectado y convertirse en el punto de inicio de un incidente de seguridad de mayor alcance.

Uno de los principales impactos corresponde a la obtención de ejecución remota de código (Remote Code Execution – RCE), que permite al actor de amenaza ejecutar instrucciones arbitrarias sobre el servidor utilizando los privilegios del proceso comprometido. Esta capacidad facilita la instalación de herramientas maliciosas, la modificación de archivos del

sistema, la creación de mecanismos de persistencia y la ejecución de actividades destinadas a mantener el acceso no autorizado dentro del entorno tecnológico de la organización.

Una vez comprometido el servidor, el atacante puede desplegar **web shells**, herramientas de administración remota o malware especializado que le permitan conservar el acceso incluso después de reiniciar el servicio o finalizar la sesión inicial. Estos mecanismos de persistencia pueden permanecer activos durante períodos prolongados si la organización no realiza actividades de búsqueda de amenazas (Threat Hunting) o análisis forense, incrementando el riesgo de que el incidente evolucione sin ser detectado.

La información almacenada en Microsoft SharePoint constituye otro de los principales objetivos para los actores de amenaza. Dependiendo de la implementación realizada por cada organización, la plataforma puede contener documentos administrativos, contratos, procedimientos institucionales, información financiera, documentación jurídica, políticas internas, registros de auditoría, proyectos estratégicos, credenciales de configuración, archivos de respaldo y otros activos de información cuya divulgación o alteración podría generar afectaciones operacionales, económicas, legales y reputacionales.

En las entidades del sector salud, la afectación puede ser aún mayor debido a que SharePoint suele utilizarse para gestionar procedimientos clínicos, protocolos asistenciales, documentación del Sistema Obligatorio de Garantía de Calidad, manuales institucionales, registros administrativos, investigaciones, documentación relacionada con la atención de pacientes e información asociada con plataformas clínicas. La exposición o alteración de estos documentos puede afectar la prestación de los servicios de salud, generar incumplimientos regulatorios y comprometer la confianza en los procesos institucionales.

Otra consecuencia relevante corresponde al robo de credenciales y tokens de autenticación. Los actores de amenaza pueden aprovechar el acceso al servidor para obtener credenciales almacenadas, extraer información de configuración, capturar sesiones activas o acceder a secretos utilizados por aplicaciones integradas. Esta información puede ser utilizada posteriormente para comprometer otros sistemas corporativos, elevar privilegios o mantener acceso persistente a la infraestructura tecnológica.

La explotación también facilita el desarrollo de actividades de reconocimiento interno. Un atacante con acceso al servidor puede identificar usuarios, grupos de seguridad, servidores

conectados, bases de datos, recursos compartidos, servicios de autenticación y aplicaciones empresariales integradas. Esta información permite planificar ataques posteriores dirigidos contra activos de mayor valor estratégico, incrementando la probabilidad de movimiento lateral dentro de la red institucional.

Desde la perspectiva de la continuidad del negocio, un servidor SharePoint comprometido puede afectar significativamente la disponibilidad de servicios utilizados diariamente por el personal asistencial, administrativo y directivo. La indisponibilidad de la plataforma puede impedir el acceso a procedimientos institucionales, documentación clínica, formularios, repositorios documentales y otros recursos esenciales para el desarrollo de las actividades operativas, obligando a implementar procedimientos alternativos que disminuyen la eficiencia y aumentan el riesgo operativo.

En escenarios más avanzados, estas vulnerabilidades pueden ser utilizadas como punto de entrada para campañas de ransomware. Después de obtener acceso inicial mediante la explotación de SharePoint, los actores de amenaza pueden desplazarse hacia otros servidores, comprometer controladores de dominio, cifrar información crítica y afectar simultáneamente múltiples servicios tecnológicos de la organización. Este tipo de incidentes puede ocasionar interrupciones prolongadas en la prestación de servicios de salud, pérdida de información y elevados costos asociados a la recuperación de la infraestructura.

Desde el punto de vista regulatorio, el compromiso de un servidor SharePoint que procese datos personales o información clínica puede derivar en incidentes con implicaciones relacionadas con la protección de datos personales, la confidencialidad de la información en salud y el cumplimiento de la normativa colombiana aplicable. Dependiendo del alcance del incidente, la organización podría verse obligada a activar sus procedimientos de gestión de incidentes de seguridad, realizar análisis de impacto, notificar a las autoridades competentes y ejecutar acciones correctivas orientadas a restablecer las condiciones de seguridad de la plataforma.

En términos generales, la explotación de estas vulnerabilidades puede permitir a un actor de amenaza:

- Obtener ejecución remota de código sobre servidores Microsoft SharePoint.
- Instalar web shells y otros mecanismos de persistencia.

- Ejecutar comandos arbitrarios en el servidor comprometido.
- Acceder, modificar o eliminar información almacenada en la plataforma.
- Robar credenciales, tokens de autenticación y archivos de configuración.
- Realizar reconocimiento de la infraestructura tecnológica institucional.
- Desplazarse lateralmente hacia otros activos de la organización.
- Utilizar el servidor comprometido como punto de apoyo para campañas de ransomware o exfiltración de información.
- Interrumpir procesos críticos soportados por Microsoft SharePoint.
- Comprometer la confidencialidad, integridad y disponibilidad de la información institucional y de los servicios digitales del sector salud.

La explotación de estas vulnerabilidades debe considerarse un riesgo de alta prioridad, especialmente en organizaciones que exponen servidores SharePoint a Internet o que aún no han aplicado las actualizaciones de seguridad y las medidas de endurecimiento recomendadas por Microsoft y CISA.

Modo de explotación del ataque

Fase 1 – Reconocimiento e identificación de servidores Microsoft SharePoint expuestos

La cadena de ataque inicia con actividades de reconocimiento orientadas a identificar servidores Microsoft SharePoint accesibles desde Internet o desde segmentos internos de la infraestructura tecnológica. Durante esta fase, el actor de amenaza busca determinar qué organizaciones utilizan versiones vulnerables de SharePoint y cuáles presentan condiciones que permitan la explotación de las vulnerabilidades recientemente divulgadas.

Para ello, el atacante emplea herramientas de descubrimiento de activos, motores de búsqueda especializados, plataformas de inteligencia de fuentes abiertas (OSINT), servicios de identificación de tecnologías expuestas y técnicas de fingerprinting que permiten identificar la versión del servidor, los servicios publicados, la configuración del servidor web IIS y otros componentes asociados a la plataforma.

En algunos casos, los actores de amenaza automatizan este proceso mediante scripts que recorren grandes bloques de direcciones IP en busca de servidores SharePoint vulnerables, reduciendo considerablemente el tiempo necesario para identificar objetivos potenciales.

Durante esta fase pueden desarrollarse actividades como:

- Identificación de servidores Microsoft SharePoint expuestos a Internet.
- Fingerprinting de versiones de SharePoint e IIS.
- Enumeración de servicios web disponibles.
- Identificación de portales institucionales.
- Descubrimiento de directorios y aplicaciones virtuales.
- Identificación de mecanismos de autenticación implementados.
- Priorización de servidores potencialmente vulnerables.

El objetivo de esta fase consiste en seleccionar los servidores con mayor probabilidad de ser comprometidos.

Fase 2 – Validación de la vulnerabilidad y preparación del entorno de explotación

Una vez identificado el servidor objetivo, el actor de amenaza valida si la instancia de SharePoint es susceptible de explotación. Para ello realiza solicitudes cuidadosamente construidas que permiten determinar la versión instalada, confirmar la presencia de la vulnerabilidad y verificar que el servidor responde conforme al comportamiento esperado por el exploit.

En esta etapa el atacante prepara la infraestructura desde la cual ejecutará el ataque, incluyendo servidores de comando y control (C2), herramientas de explotación, proxys, redes privadas virtuales (VPN) o infraestructura comprometida previamente para ocultar el origen de las conexiones.

Cuando existen exploits públicos o pruebas de concepto (Proof of Concept – PoC), estos suelen adaptarse para automatizar el proceso de explotación y facilitar ataques contra múltiples organizaciones de forma simultánea.

Las actividades desarrolladas durante esta fase pueden incluir:

- Validación de la versión instalada de SharePoint.
- Confirmación de la vulnerabilidad.

- Preparación del exploit.
- Configuración de la infraestructura de ataque.
- Verificación de conectividad.
- Configuración de herramientas de post-explotación.
- Automatización del proceso de explotación.

El objetivo consiste en garantizar que el ataque pueda ejecutarse con la mayor probabilidad de éxito y el menor riesgo de ser detectado.

Fase 3 – Explotación de la vulnerabilidad y obtención de ejecución remota de código

Confirmada la existencia de la vulnerabilidad, el actor de amenaza ejecuta el exploit diseñado para aprovechar la falla presente en Microsoft SharePoint. Como resultado, logra ejecutar código arbitrario dentro del servidor afectado utilizando el contexto de seguridad asociado al servicio comprometido.

La ejecución remota de código constituye el punto de inflexión del ataque, ya que permite al atacante interactuar directamente con el sistema operativo, crear archivos, modificar configuraciones, ejecutar procesos, instalar componentes adicionales y preparar el entorno para fases posteriores del compromiso.

Dependiendo de la configuración del servidor y del nivel de privilegios obtenido, esta fase puede completarse en pocos segundos sin generar interrupciones visibles para los usuarios legítimos de la plataforma.

Las actividades desarrolladas incluyen:

- Ejecución del exploit.
- Creación del acceso inicial.
- Ejecución de comandos arbitrarios.
- Validación del contexto de ejecución.
- Identificación del nivel de privilegios obtenido.
- Verificación del acceso persistente.
- Preparación del servidor para actividades posteriores.

El objetivo consiste en obtener control operativo sobre el servidor SharePoint comprometido.

Fase 4 – Establecimiento de persistencia e instalación de componentes maliciosos

Una vez obtenido el acceso inicial al servidor SharePoint, el actor de amenaza desarrolla actividades orientadas a mantener el control del sistema durante el mayor tiempo posible, incluso si la vulnerabilidad utilizada para el acceso inicial es corregida posteriormente. Para ello, implementa mecanismos de persistencia que le permitan recuperar el acceso sin necesidad de ejecutar nuevamente el proceso de explotación.

Una de las técnicas más utilizadas consiste en la instalación de web shells, las cuales son archivos maliciosos alojados dentro del servidor web que permiten ejecutar comandos remotos mediante solicitudes HTTP o HTTPS aparentemente legítimas. Estas herramientas proporcionan al atacante una interfaz permanente para administrar el servidor, cargar o descargar archivos, ejecutar scripts, modificar contenido y desplegar herramientas adicionales. Adicionalmente, el actor de amenaza puede crear tareas programadas, instalar servicios, modificar configuraciones del sistema operativo o incorporar herramientas de administración remota (RAT), con el propósito de garantizar múltiples mecanismos de acceso en caso de que alguno de ellos sea identificado y eliminado.

Las actividades desarrolladas durante esta fase pueden incluir:

- Instalación de web shells en el servidor SharePoint.
- Creación de mecanismos de persistencia.
- Implementación de herramientas de administración remota.
- Modificación de configuraciones del sistema operativo.
- Creación de tareas programadas o servicios.
- Carga de herramientas de post-explotación.
- Verificación de los mecanismos de acceso persistente.

El objetivo consiste en garantizar que el actor de amenaza pueda mantener el acceso al servidor comprometido durante un periodo prolongado y continuar desarrollando actividades maliciosas sin depender nuevamente de la vulnerabilidad inicial.

Fase 5 – Reconocimiento interno y movimiento lateral

Con el servidor SharePoint bajo su control, el atacante inicia actividades de reconocimiento sobre la infraestructura tecnológica de la organización. El propósito de esta fase es identificar otros activos de alto valor, comprender la arquitectura de la red y localizar sistemas que puedan ser comprometidos posteriormente.

Durante este proceso se recopila información sobre usuarios, grupos de Active Directory, servidores de archivos, controladores de dominio, bases de datos, aplicaciones corporativas, recursos compartidos, sistemas de respaldo, plataformas de virtualización y demás componentes conectados al entorno institucional.

Cuando el servidor SharePoint mantiene relaciones de confianza con otros sistemas, el actor de amenaza puede utilizar las credenciales obtenidas o los privilegios disponibles para desplazarse lateralmente hacia nuevos equipos, ampliando progresivamente el alcance del incidente.

Las actividades desarrolladas durante esta fase pueden incluir:

- Enumeración de usuarios y grupos de Active Directory.
- Identificación de servidores y aplicaciones corporativas.
- Descubrimiento de recursos compartidos.
- Recolección de credenciales y tokens de autenticación.
- Identificación de bases de datos y servicios críticos.
- Movimiento lateral hacia otros servidores.
- Priorización de activos de alto valor para fases posteriores del ataque.

El objetivo consiste en ampliar el acceso dentro de la infraestructura tecnológica y preparar el compromiso de sistemas adicionales.

Fase 6 – Acceso a la información y compromiso de activos críticos

Una vez identificado el entorno tecnológico, el actor de amenaza dirige sus esfuerzos hacia los activos de mayor valor para la organización. En el contexto del sector salud, esto puede incluir repositorios documentales, información administrativa, documentación contractual, procedimientos institucionales, bases de datos, aplicaciones clínicas y otros sistemas que procesen información sensible.

Dependiendo de los privilegios obtenidos, el atacante puede consultar, copiar, modificar o eliminar documentos almacenados en SharePoint, acceder a información contenida en bibliotecas documentales, descargar archivos estratégicos o utilizar las credenciales recopiladas para comprometer otros sistemas corporativos.

En campañas dirigidas, esta fase también puede incluir la preparación de información para su posterior exfiltración o la manipulación deliberada de documentos con el propósito de afectar la operación institucional.

Las actividades desarrolladas durante esta fase pueden incluir:

- Acceso a bibliotecas y repositorios documentales.
- Descarga de documentos institucionales.
- Obtención de información sensible.
- Compromiso de aplicaciones integradas con SharePoint.
- Modificación o eliminación de información.
- Preparación de datos para su exfiltración.
- Identificación de activos adicionales de interés.

El objetivo consiste en obtener acceso a información estratégica que permita maximizar el impacto del incidente sobre la organización.

Fase 7 – Exfiltración de información y afectación de la operación institucional

En la fase final, el actor de amenaza materializa los objetivos de la campaña. Dependiendo de su motivación, puede exfiltrar información sensible, desplegar ransomware, destruir evidencia,

alterar documentos institucionales o mantener el acceso para futuras operaciones de espionaje o sabotaje.

La información extraída puede incluir documentos administrativos, información financiera, registros de auditoría, procedimientos institucionales, documentación técnica y otros activos de información cuyo valor estratégico puede ser aprovechado para extorsión, fraude o campañas de inteligencia.

En escenarios de ransomware, el acceso obtenido mediante SharePoint puede utilizarse para cifrar información almacenada en servidores conectados, afectar servicios corporativos y generar interrupciones significativas en la prestación de los servicios de salud.

Las actividades desarrolladas durante esta fase pueden incluir:

- Exfiltración de información institucional.
- Despliegue de ransomware u otro malware.
- Eliminación o alteración de evidencias.
- Manipulación de documentos críticos.
- Interrupción de servicios soportados por SharePoint.
- Mantenimiento del acceso para futuras operaciones.
- Encubrimiento de las actividades realizadas.

El objetivo consiste en maximizar el impacto del compromiso sobre la organización, obteniendo beneficios económicos, estratégicos o de inteligencia, y afectando la continuidad de los servicios tecnológicos que soportan la atención y la gestión del sector salud.

Vulnerabilidades asociadas

Las campañas recientes dirigidas contra Microsoft SharePoint demuestran que los actores de amenaza aprovechan cadenas de explotación compuestas por múltiples vulnerabilidades para obtener acceso inicial, ejecutar código de forma remota y mantener persistencia sobre los servidores comprometidos. La combinación de estas debilidades incrementa significativamente la probabilidad de compromiso exitoso cuando las organizaciones no aplican oportunamente las actualizaciones de seguridad o mantienen configuraciones inseguras.

En este contexto, CISA y Microsoft han recomendado a las organizaciones identificar de manera prioritaria los servidores Microsoft SharePoint implementados en entornos locales (On-Premises), validar la versión instalada, aplicar las actualizaciones de seguridad disponibles y adoptar medidas de endurecimiento (hardening) que reduzcan la superficie de ataque y dificulten la explotación de estas vulnerabilidades.

CVE-2025-53770 – Ejecución remota de código (Remote Code Execution – RCE)

Corresponde a una vulnerabilidad crítica que permite a un actor de amenaza ejecutar código arbitrario sobre servidores Microsoft SharePoint sin requerir autenticación previa, bajo determinadas condiciones. La explotación exitosa puede proporcionar acceso inicial al servidor, facilitar la instalación de componentes maliciosos y servir como punto de partida para el compromiso de otros activos tecnológicos de la organización.

Su criticidad radica en que permite comprometer directamente la plataforma SharePoint y ejecutar instrucciones con los privilegios asociados al servicio afectado, facilitando la instalación de web shells, herramientas de administración remota y mecanismos de persistencia.

CVE-2025-53771 – Divulgación de información (Information Disclosure)

Esta vulnerabilidad permite que un actor de amenaza obtenga acceso a información sensible que puede ser utilizada para facilitar fases posteriores del ataque. La información expuesta puede contribuir al reconocimiento del entorno, a la identificación de configuraciones internas y al desarrollo de cadenas de explotación más complejas.

Aunque por sí sola no implica el compromiso completo del servidor, su explotación puede incrementar significativamente la probabilidad de éxito cuando es utilizada conjuntamente con vulnerabilidades de ejecución remota de código.

Configuraciones inseguras de Microsoft SharePoint

Además de las vulnerabilidades identificadas mediante CVE, diversas configuraciones inseguras pueden incrementar la superficie de ataque de la plataforma. Entre las más relevantes se encuentran:

- Exposición de servidores SharePoint directamente a Internet.
- Uso de cuentas de servicio con privilegios excesivos.
- Falta de aplicación oportuna de actualizaciones de seguridad.
- Configuración inadecuada de IIS.
- Deficiencias en la autenticación multifactor para cuentas administrativas.
- Controles insuficientes sobre PowerShell y administración remota.

Estas condiciones no constituyen vulnerabilidades por sí mismas, pero aumentan considerablemente el riesgo de explotación y facilitan el compromiso de la infraestructura tecnológica.

Explotación mediante cadenas de ataque

Los incidentes recientes evidencian que los actores de amenaza rara vez utilizan una única vulnerabilidad. En su lugar, combinan vulnerabilidades de ejecución remota de código, divulgación de información, configuraciones inseguras y herramientas de post-explotación para obtener acceso persistente, escalar privilegios y desplazarse lateralmente hacia otros sistemas de la organización.

En consecuencia, la mitigación efectiva no debe limitarse a la instalación de actualizaciones de seguridad. También requiere fortalecer la configuración de Microsoft SharePoint, implementar controles de monitoreo continuo, restringir la exposición de los servidores a Internet, aplicar el principio de mínimo privilegio y adoptar las recomendaciones de hardening publicadas por Microsoft y CISA, reduciendo así la probabilidad de compromiso de la plataforma y de los activos críticos del sector salud.

Detección

La identificación temprana de intentos de explotación contra Microsoft SharePoint resulta fundamental para reducir el impacto de un incidente de seguridad. Debido a que las campañas recientes han demostrado un alto grado de automatización, las organizaciones deben fortalecer sus capacidades de monitoreo continuo, correlación de eventos y búsqueda proactiva de amenazas (Threat Hunting), prestando especial atención a los servidores SharePoint expuestos a Internet.

Las actividades de detección deben orientarse a identificar comportamientos anómalos que indiquen la explotación de vulnerabilidades, la ejecución de código no autorizado, la instalación de componentes maliciosos o la utilización de mecanismos de persistencia. Para ello, es recomendable integrar los registros de Microsoft SharePoint, Internet Information Services (IIS), Windows Server y las soluciones de seguridad corporativas dentro de una plataforma SIEM que permita correlacionar eventos y generar alertas oportunas.

Los equipos responsables de la seguridad de la información deben monitorear, entre otros, los siguientes indicadores:

- Solicitudes HTTP o HTTPS inusuales dirigidas a aplicaciones SharePoint.
- Incremento anormal de errores 500, 401, 403 o 404 en IIS.
- Creación inesperada de archivos ASPX, DLL, ASHX o scripts dentro de los directorios de SharePoint.
- Aparición de web shells o archivos ejecutables no autorizados.
- Ejecución de procesos anómalos por parte de **w3wp.exe**, **OWSTIMER.EXE**, **powershell.exe**, **cmd.exe**, **cscript.exe** o **wscript.exe**.
- Creación de tareas programadas, servicios o cuentas administrativas sin autorización.
- Conexiones salientes del servidor hacia direcciones IP externas no habituales.
- Transferencias masivas de información desde bibliotecas documentales.
- Cambios inesperados en configuraciones de IIS o SharePoint.
- Incremento inusual en la actividad de autenticación o acceso privilegiado.

Asimismo, es recomendable revisar periódicamente los registros generados por:

- Microsoft SharePoint ULS Logs.

- Internet Information Services (IIS).
- Windows Event Viewer.
- Microsoft Defender for Endpoint.
- Microsoft Defender XDR.
- Microsoft Sentinel.
- Sysmon.
- Active Directory.
- Microsoft Entra ID.
- Soluciones EDR y XDR implementadas por la organización.

En actividades de Threat Hunting, resulta conveniente verificar la existencia de archivos recientemente creados dentro de los directorios de SharePoint, identificar procesos iniciados por el servicio web que normalmente no deberían ejecutarse y validar conexiones de red establecidas desde el servidor hacia destinos externos desconocidos. También debe revisarse la presencia de comandos PowerShell codificados, ejecución de utilidades administrativas fuera de los horarios habituales y modificaciones no autorizadas en bibliotecas documentales o archivos de configuración.

Desde la perspectiva del sector salud, cualquier comportamiento anómalo sobre servidores SharePoint que soporten procesos relacionados con Historia Clínica Electrónica (HCE), gestión documental, interoperabilidad, sistemas administrativos o repositorios institucionales debe ser tratado como un posible incidente de seguridad y activar los procedimientos establecidos por la organización para su análisis, contención y erradicación.

Prevención y Mitigación

Con el propósito de reducir la probabilidad de explotación de las vulnerabilidades que afectan a Microsoft SharePoint, las organizaciones del sector salud deben implementar medidas técnicas, administrativas y operacionales orientadas a disminuir la superficie de ataque y fortalecer la protección de los servidores que soportan esta plataforma.

Como medida prioritaria, se recomienda aplicar inmediatamente las actualizaciones de seguridad publicadas por Microsoft para las versiones afectadas de SharePoint Server. La actualización oportuna constituye el mecanismo más efectivo para eliminar las vulnerabilidades conocidas y evitar que sean aprovechadas por actores de amenaza.

Adicionalmente, CISA recomienda implementar un proceso de hardening sobre los servidores SharePoint que contemple, como mínimo, las siguientes acciones:

- Mantener Microsoft SharePoint completamente actualizado.
- Restringir la exposición de SharePoint a Internet cuando no sea estrictamente necesario.
- Implementar segmentación de red para aislar los servidores SharePoint de otros segmentos críticos.
- Aplicar el principio de mínimo privilegio a cuentas de servicio y cuentas administrativas.
- Habilitar autenticación multifactor (MFA) para todas las cuentas con privilegios elevados.
- Restringir el acceso administrativo únicamente desde estaciones de administración autorizadas.
- Revisar periódicamente los permisos asignados sobre bibliotecas y sitios SharePoint.
- Fortalecer la configuración de Internet Information Services (IIS).
- Implementar monitoreo continuo mediante soluciones SIEM, EDR y XDR.
- Proteger los servidores mediante soluciones antimalware con capacidades de detección de comportamiento.
- Realizar copias de seguridad periódicas verificando su integridad y posibilidad de recuperación.
- Ejecutar análisis periódicos de vulnerabilidades sobre la infraestructura SharePoint.
- Eliminar componentes, extensiones o servicios que no sean necesarios para la operación.
- Revisar permanentemente los registros de auditoría y eventos de seguridad.
- Establecer procedimientos de respuesta específicos para servidores SharePoint comprometidos.

En organizaciones del sector salud, estas medidas deben complementarse con la revisión de las integraciones existentes entre SharePoint y otros sistemas críticos, verificando que únicamente se mantengan habilitadas aquellas conexiones estrictamente necesarias para la operación institucional.

Finalmente, se recomienda realizar ejercicios periódicos de evaluación de la postura de seguridad, pruebas de penetración controladas y actividades de Threat Hunting que permitan identificar oportunamente configuraciones inseguras, indicadores de compromiso y posibles mecanismos de persistencia antes de que puedan ser utilizados para afectar la disponibilidad de los servicios tecnológicos o comprometer información sensible de pacientes e instituciones.

Respuesta ante un incidente

En caso de identificar indicios de explotación o compromiso de un servidor Microsoft SharePoint, las organizaciones del sector salud deberán activar de manera inmediata sus procedimientos de gestión de incidentes de seguridad de la información, con el propósito de contener la amenaza, preservar las evidencias, limitar el alcance del incidente y restablecer la operación de forma segura.

La respuesta inicial debe orientarse a confirmar el compromiso del servidor mediante el análisis de los registros de auditoría, eventos del sistema operativo, registros de IIS, registros de Microsoft SharePoint y la información recopilada por las soluciones EDR, XDR y SIEM implementadas por la organización. Esta validación permitirá determinar el alcance del incidente, identificar los sistemas afectados y priorizar las acciones de contención.

Como primera medida de contención, se recomienda aislar el servidor comprometido de la red corporativa cuando la continuidad del servicio lo permita, evitando que el actor de amenaza continúe ejecutando actividades de reconocimiento, movimiento lateral, exfiltración de información o instalación de componentes adicionales. Si el aislamiento inmediato no es viable debido al impacto operacional, deberán implementarse controles temporales que restrinjan las comunicaciones del servidor únicamente a los servicios estrictamente necesarios para la atención del incidente.

Posteriormente, la organización deberá realizar un análisis técnico orientado a identificar la presencia de web shells, herramientas de administración remota no autorizadas, archivos sospechosos, tareas programadas, servicios instalados recientemente, cuentas creadas sin autorización y cualquier otro mecanismo de persistencia implementado por el actor de amenaza. Esta actividad debe complementarse con la revisión de procesos en ejecución, conexiones de red activas y modificaciones recientes sobre archivos de configuración de SharePoint e IIS.

Durante el proceso de erradicación deberán eliminarse todos los componentes maliciosos identificados, aplicar las actualizaciones de seguridad publicadas por Microsoft, implementar las medidas de hardening recomendadas por CISA, restablecer las configuraciones seguras del servidor y verificar la integridad de los archivos críticos antes de permitir nuevamente su operación.

Como medida preventiva adicional, se recomienda revocar y restablecer las credenciales de las cuentas administrativas, cuentas de servicio y demás identidades que hayan podido verse comprometidas durante el incidente. Igualmente, deberán revisarse los permisos asignados en SharePoint, Active Directory, Microsoft Entra ID y demás plataformas integradas, con el fin de identificar posibles modificaciones realizadas por el actor de amenaza.

Una vez finalizadas las actividades de erradicación, la organización deberá recuperar el servicio utilizando respaldos verificados cuando sea necesario, validar el correcto funcionamiento de la plataforma y mantener un monitoreo reforzado durante un periodo prudencial para detectar posibles intentos de reinfección o mecanismos de persistencia que no hayan sido identificados durante la investigación inicial.

Recomendaciones

Con el propósito de reducir el riesgo de explotación de las vulnerabilidades que afectan a Microsoft SharePoint, el CSIRT Salud recomienda a las entidades del sector salud implementar las siguientes medidas de seguridad:

- Identificar todos los servidores Microsoft SharePoint implementados en la organización, incluyendo ambientes de producción, pruebas y contingencia.
- Aplicar inmediatamente las actualizaciones de seguridad publicadas por Microsoft para las versiones afectadas.
- Implementar las medidas de hardening recomendadas por CISA para Microsoft SharePoint e Internet Information Services (IIS).
- Verificar que no existan servidores SharePoint expuestos directamente a Internet cuando esta condición no sea estrictamente necesaria para la operación institucional.
- Restringir el acceso administrativo mediante listas de control de acceso, segmentación de red y estaciones de administración dedicadas.
- Habilitar autenticación multifactor para todas las cuentas con privilegios administrativos.
- Revisar periódicamente los permisos asignados a usuarios, grupos y cuentas de servicio bajo el principio de mínimo privilegio.
- Implementar monitoreo continuo sobre los servidores SharePoint utilizando soluciones SIEM, EDR y XDR.

- Realizar actividades periódicas de búsqueda proactiva de amenazas (Threat Hunting) para identificar indicadores de compromiso o mecanismos de persistencia.
- Revisar diariamente los registros de IIS, Microsoft SharePoint, Windows Server y Active Directory en busca de comportamientos anómalos.
- Ejecutar análisis de vulnerabilidades y pruebas de penetración sobre la infraestructura SharePoint como parte del programa de gestión de vulnerabilidades de la organización.
- Mantener respaldos actualizados, protegidos y verificados mediante pruebas periódicas de restauración.
- Capacitar a los equipos responsables de infraestructura, administración de SharePoint y ciberseguridad sobre las técnicas de explotación recientemente observadas y las medidas de respuesta recomendadas.
- Actualizar los procedimientos de gestión de incidentes para incorporar escenarios específicos relacionados con el compromiso de plataformas de colaboración y gestión documental.
- Mantener un proceso permanente de seguimiento a los boletines de seguridad publicados por Microsoft, CISA y el CSIRT Salud para implementar oportunamente nuevas medidas de mitigación frente a vulnerabilidades emergentes.

Estas recomendaciones contribuirán a reducir la superficie de ataque, fortalecer la resiliencia de la infraestructura tecnológica y proteger la información crítica administrada por las organizaciones del sector salud frente a campañas dirigidas contra plataformas Microsoft SharePoint.

Conclusiones

Las recientes campañas de explotación dirigidas contra Microsoft SharePoint evidencian que esta plataforma continúa siendo un objetivo prioritario para actores de amenaza debido a su amplia adopción en entornos corporativos y a la información crítica que almacena y procesa. La explotación de vulnerabilidades de ejecución remota de código puede proporcionar acceso inicial a la infraestructura tecnológica, facilitar la instalación de mecanismos de persistencia y servir como punto de partida para comprometer otros activos estratégicos de la organización.

En las entidades del sector salud, el riesgo adquiere una mayor relevancia debido a que Microsoft SharePoint soporta procesos relacionados con la gestión documental, la administración institucional, los sistemas integrados de gestión, la interoperabilidad y, en

algunos casos, aplicaciones que procesan información clínica o se encuentran integradas con plataformas críticas para la prestación de los servicios de salud. El compromiso de estos servidores puede afectar la confidencialidad, integridad y disponibilidad de la información institucional, además de impactar la continuidad de los procesos asistenciales y administrativos.

La publicación de las recomendaciones de endurecimiento (hardening) por parte de la Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA) pone de manifiesto que la aplicación de actualizaciones de seguridad, aunque indispensable, no constituye por sí sola una medida suficiente para reducir el riesgo de explotación. La protección efectiva de Microsoft SharePoint requiere la implementación de una estrategia de defensa en profundidad que incluya la reducción de la superficie de ataque, el fortalecimiento de las configuraciones de seguridad, el monitoreo continuo, la gestión oportuna de vulnerabilidades y la adopción del principio de mínimo privilegio.

De igual manera, resulta fundamental que las organizaciones mantengan una capacidad permanente de detección y respuesta frente a actividades anómalas sobre los servidores SharePoint, mediante el monitoreo de registros, la búsqueda proactiva de indicadores de compromiso, la validación periódica de la integridad de los sistemas y la ejecución de ejercicios de Threat Hunting que permitan identificar oportunamente posibles mecanismos de persistencia o intentos de explotación.

El **CSIRT Salud** recomienda a todas las entidades del sector salud identificar los servidores Microsoft SharePoint implementados dentro de su infraestructura tecnológica, verificar la aplicación de las actualizaciones de seguridad publicadas por Microsoft, implementar las medidas de hardening recomendadas por CISA, fortalecer los mecanismos de monitoreo y respuesta a incidentes, y mantener un proceso continuo de evaluación de la postura de seguridad. La adopción oportuna de estas acciones contribuirá a reducir la probabilidad de compromiso de la plataforma, proteger la información crítica del sector salud y fortalecer la resiliencia de las organizaciones frente a amenazas dirigidas contra servicios de colaboración y gestión documental.

Fuentes:

- <https://msrc.microsoft.com/>
- <https://msrc.microsoft.com/update-guide>
- <https://learn.microsoft.com/sharepoint/>
- <https://learn.microsoft.com/sharepoint/security-for-sharepoint-server>
- <https://www.cisa.gov/>
- <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- <https://www.cisa.gov/news-events/cybersecurity-advisories>
- <https://attack.mitre.org/>
- <https://www.cve.org/>
- <https://nvd.nist.gov/>
- <https://learn.microsoft.com/defender-xdr/>
- <https://learn.microsoft.com/defender-endpoint/>
- <https://learn.microsoft.com/azure/sentinel/>
- <https://learn.microsoft.com/iis/>
- <https://securityonline.info/cisa-sharepoint-hardening/>

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.