Alerta de

Seguridad

Vulnerabilidad Crítica
Zero-Day en Microsoft SharePoint Server

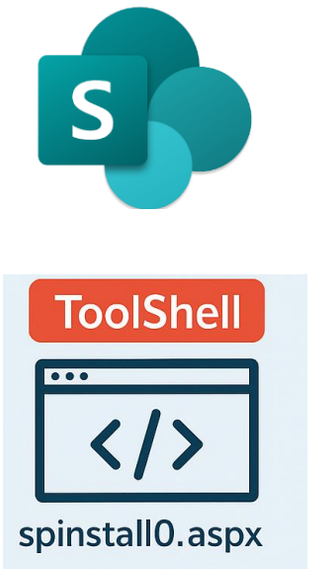
COLCERT AL-20250720-067

TLP:CLEAR

Microsoft ha confirmado la explotación activa de la vulnerabilidad **zero-day CVE-2025-53770** en servidores SharePoint on-premises, la cual permite ejecución remota de código (RCE) sin autenticación mediante una cadena de ataques conocida como "ToolShell".

Esta **amenaza crítica ya ha comprometido múltiples servidores a nivel global** mediante la instalación de web shells como spinstall0.aspx, facilitando el robo de secretos criptográficos. Como no existe parche aún disponible, se recomienda aplicar mitigaciones inmediatas: habilitar AMSI y Microsoft Defender en los servidores, buscar indicadores de compromiso como accesos sospechosos a ToolPane.aspx, y aislar sistemas potencialmente afectados.

Además, debe iniciarse un análisis de compromiso completo, rotar secretos criptográficos, y preparar la infraestructura para el despliegue inmediato del parche cuando esté disponible.



Descripción:

Identificador CVE: CVE-2025-53770
Tipo de Vulnerabilidad: Ejecución Remota de Código (RCE) por deserialización de datos no confiables. Puntuación CVSS v3.1: 9.8 (Crítica)
Productos Afectados: Microsoft SharePoint Server 2016, 2019, y Subscription Edition (instalaciones locales).
Productos NO Afectados: SharePoint Online (Microsoft 365) no se ve afectado.

¿Cómo se Explota esta Vulnerabilidad?

Esta falla es una vulnerabilidad de deserialización. En términos sencillos, cuando SharePoint procesa ciertos datos que provienen de una fuente externa (como una solicitud de red), no valida o "limpia" adecuadamente esa información. **Un atacante puede enviar datos maliciosos y especialmente diseñados al servidor de SharePoint.** Debido a este error en el manejo de la información, el servidor interpreta estos datos como comandos legítimos y ejecuta el código proporcionado por el atacante, logrando así la ejecución remota de código sin necesidad de autenticación.

Microsoft ha identificado esta vulnerabilidad como una variante de CVE-2025-49706, que también es una falla de SharePoint. **Esto sugiere que los atacantes han encontrado una nueva forma de bypass o explotar una debilidad relacionada.**

Análisis de riesgo por categoría

Riesgo	Impacto	Probabilidad	Acción recomendada
Robo de secretos	Alto	Alta	Rotar certificados y claves
Persistencia del atacante	Alto	Media	Buscar web shells y backdoors
Movimiento lateral	Crítico	Media-Alta	Monitoreo y segmentación
Exposición pública RCE	Crítico	Alta	Aislar de Internet y aplicar mitigaciones

El análisis de riesgo por categoría permite priorizar la respuesta ante la vulnerabilidad CVE-2025-53770 al identificar impactos clave: compromiso de secretos criptográficos, persistencia mediante web shells, movimiento lateral dentro de la red y ejecución remota sin autenticación. Estos vectores representan riesgos críticos que requieren acciones inmediatas como rotación de claves, monitoreo de IoC y posible aislamiento de servidores expuestos para contener la amenaza de forma efectiva.

MITRE ATT&CK

Técnica MITRE	ID	Descripción
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059.001	PowerShell
Persistence	T1505.003	Web Shell
Defense Evasion	T1036	Masquerading
Exfiltration	T1041	Exfiltration Over C2 Channel

Mapear esta amenaza con MITRE ATT&CK permite identificar técnicas clave como uso de web shells (T1505.003), PowerShell (T1059.001) y explotación de servicios expuestos (T1190), facilitando detecciones basadas en comportamiento y respuestas más efectivas.

Este enfoque fortalece la defensa ante movimientos laterales, exfiltración (T1041) y evasión de controles (T1036).

Recomendaciones y medidas de protección Urgentes (Mientras Microsoft Libera el Parche)

Dado que Microsoft aún no ha publicado una actualización oficial, es URGENTE aplicar las siguientes mitigaciones para protegerse.

- ❑ Habilitar la Integración de interfaz de Análisis Antimalware AMSI y Desplegar Microsoft Defender Antivirus (o EDR similar).
- ❑ **Prioridad Alta:** Asegúrese de que la AMSI esté habilitada en sus servidores SharePoint. AMSI puede ayudar a detener los ataques de ejecución de código antes de que impacten.
- ❑ **Verificación:** AMSI está habilitado por defecto si tiene aplicadas las actualizaciones de seguridad de septiembre de 2023 (para SharePoint Server 2016/2019) o la actualización de características de la Versión 23H2 (para SharePoint Server Subscription Edition). Verifique la instalación de estas actualizaciones.
- ❑ **Despliegue de Antivirus/EDR:** Asegúrese de que Microsoft Defender Antivirus (o su solución de detección y respuesta de endpoints (EDR) equivalente) esté desplegado y completamente actualizado en todos los servidores de SharePoint.
- ❑ **Detecciones Específicas:** Microsoft Defender Antivirus proporciona protección bajo las siguientes firmas: Exploit:Script/SuspSignoutReq.A y Trojan:Win32/HijackSharePointServer.A. Verifique que su solución EDR tenga estas detecciones.

> **Considerar la Desconexión Temporal de Internet (Si la Continuidad del Negocio lo Permite):** Para organizaciones con entornos extremadamente críticos y/o que no puedan implementar rápidamente la protección AMSI/EDR, considere desconectar temporalmente los servidores de SharePoint de Internet hasta que el parche esté disponible. Esta es una medida drástica, pero efectiva para eliminar la superficie de ataque externa.

Monitoreo Continuo de Indicadores de Compromiso (IoC)

Revisar Registros (Logs): Busque la creación del archivo spinstall0.aspx en sus servidores SharePoint, ya que este es un indicador clave de una explotación exitosa.

Alertas Específicas: Monitoree las alertas de su EDR/SIEM relacionadas con:

"Possible web shell installation"
"Possible exploitation of SharePoint server vulnerabilities"
"Suspicious IIS worker process behavior"
Bloqueos de SuspSignoutReq o HijackSharePointServer

Actividad de Procesos: Esté atento a procesos inusuales o no autorizados ejecutándose bajo las cuentas de servicio de SharePoint o el pool de aplicaciones de IIS.

Indicadores de Compromiso (IoC):

Tipo de IoC	Valor
IP sospechosa	107.191.58[.]76
IP sospechosa	104.238.159[.]149
IP sospechosa	96.9.125[.]147
IP sospechosa	96.9.125[.]227
Hash SHA-256	4a02a72aedc3356d8cb38f01f0e0b9f26ddc5ccb7c0f04a561337cf24aa84030
Hash SHA-256	b39c14becb62aeb55df7fd55c814afbb0d659687d947d917512fe67973100b70
Hash SHA-256	Fa3a74a6c015c801f5341c02be2cbdfb301c6ed60633d49fc0bc723617741af7

Fuente: CSIRT Claro

CVE Asociados y Relacionados

Es importante recordar que esta vulnerabilidad (CVE-2025-53770) es una variante o está estrechamente relacionada con CVE-2025-49706, otra vulnerabilidad de SharePoint. Asegúrese de que todas las actualizaciones y mitigaciones relacionadas con vulnerabilidades previas de SharePoint estén aplicadas.

Variante de CVE-2025-49706 (una vulnerabilidad de suplantación de identidad o "spoofing" en SharePoint que fue parcheada en el Patch Tuesday de julio de 2025).

“La explotación activa de esta vulnerabilidad permite ejecución remota sin autenticación, lo que representa un riesgo crítico que exige medidas inmediatas.”

Fuentes Oficiales

- https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770/
- https://nvd.nist.gov/vuln/detail/CVE-2025-53770
- https://www.cisa.gov/news-events/alerts/2025/07/20/microsoft-releases-guidance-exploitation-sharepoint-vulnerability-cve-2025-53770
- https://thehackernews.com/2025/07/critical-microsoft-sharepoint-flaw.html
- https://blog.segu-info.com.ar/2025/07/explotacion-masiva-de-zero-day.html

❑ **CSIRT (Computer Security Incident Response Team) Claro Colombia**