Alerta de

Seguridad

Seguimiento vulnerabilidad crítica Microsoft SharePoint

COLCERT AL-20250728-069

TLP:CLEAR

En seguimiento a nuestra Alerta de Seguridad **COLCERT AL-20250720-067**, emitida el pasado 20 de julio, queremos reiterar y ampliar la urgencia respecto a la vulnerabilidad crítica Zero-Day **CVE-2025-53770 en Microsoft SharePoint Server**. Esta falla sigue bajo **explotación activa y persistente**, con múltiples evidencias de uso por grupos estatales y actores de ransomware como **Storm-2603**.

Dado el nivel de amenaza, es crucial complementar las mitigaciones que ya les habíamos recomendado. La continua evolución de los ataques y la naturaleza de "día cero" de esta vulnerabilidad exigen una **postura de seguridad aún más proactiva y vigilante**.

Por esto, enfatizamos la **importancia crítica de validar y buscar activamente los Indicadores de Compromiso (IoCs)** que se han publicado para esta amenaza. Más allá de aplicar parches (una vez disponibles) y mitigaciones preventivas, la verificación de estos IoCs es **esencial para determinar si sus sistemas ya han sido comprometidos**. De ser así, podrán tomar acciones inmediatas de respuesta. La detección temprana de una intrusión puede ser la diferencia clave para contener un incidente y proteger eficazmente su información sensible.

Vulnerabilidad identificada

CVE	PRODUCTO	SCORE CVSS	IMPACTO	ACCIONES RECOMENDADAS
CVE-2025-53770	Versiones locales de Microsoft SharePoint Server 2016, 2019 y Subscription Edition.	**9.8**	Permite a los ciberdelincuentes ejecutar código remotamente sin autenticación, comprometiendo por completo servidores SharePoint vulnerables.	Aplicar de inmediato los parches de seguridad disponibles para SharePoint, habilitar AMSI y Microsoft Defender Antivirus en modo completo, rotar las claves criptográficas (MachineKey) tras la actualización, reiniciar IIS, y monitorear accesos sospechosos o archivos anómalos en los servidores afectados para detectar posibles compromisos.

NIVEL DE RIESGO

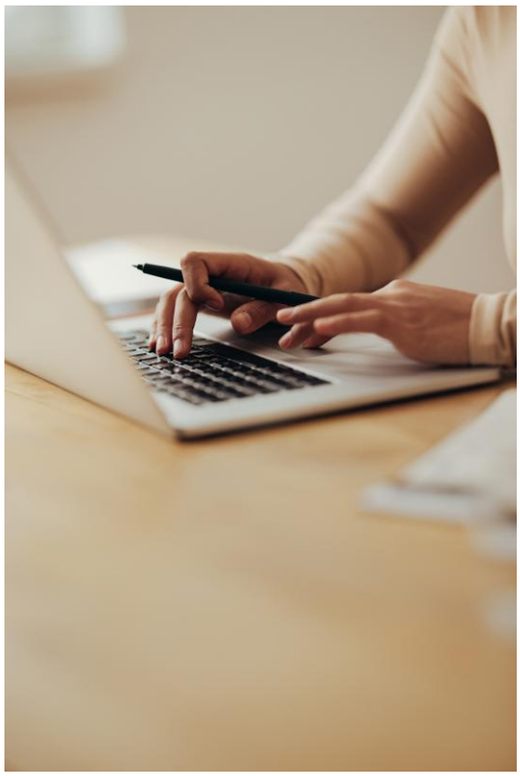
ALTO

¿Cómo se explota esta vulnerabilidad?

La vulnerabilidad CVE-2025-53770 se explota cargando un archivo .aspx malicioso (por ejemplo, spinstall0.aspx) en el servidor SharePoint sin necesidad de autenticación. El ciberdelincuente luego extrae las claves de validación y cifrado (MachineKeys) del servidor para generar vistas (__VIEWSTATE) firmadas, lo que le permite ejecutar comandos arbitrarios de forma remota con privilegios elevados, comprometiendo completamente el sistema afectado.

Herramientas de escaneo y Pruebas de Concepto (PoC)

Existen varios repositorios en GitHub relacionados con la vulnerabilidad **CVE-2025-53770**, como el del usuario hazcod, que ofrecen **herramientas de escaneo** para detectar servidores SharePoint vulnerables. Estos repositorios permiten a los equipos de seguridad verificar la exposición a esta falla crítica mediante pruebas controladas, facilitando una evaluación rápida del riesgo en entornos propios antes de posibles compromisos. A continuación se comparten algunos repositorios:



- **hxxps://github[.com/hazcod/CVE-2025-53770**
- **hxxps://github[.]com/ZephrFish/CVE-2025-53770-Scanner**

En GitHub también se encuentran disponibles varias pruebas de concepto (PoC) relacionadas con la vulnerabilidad CVE-2025-53770, las cuales demuestran de forma técnica cómo puede ser explotada en entornos SharePoint vulnerables. Estos repositorios permiten simular el ataque sin necesidad de autenticación, evidenciando el riesgo real de ejecución remota de código. Las PoC están destinadas a facilitar la evaluación de seguridad en entornos propios y apoyar acciones de mitigación proactiva por parte de los equipos de ciberseguridad. A continuación se comparten algunos repositorios:

- **hxxps://github[.]com/B1ack4sh/Blackash-CVE-2025-53770**
- **hxxps://github[.]com/soltanali0/CVE-2025-53770-Exploit**

Impacto para Colombia y la región

La vulnerabilidad **CVE-2025-53770** representa una amenaza significativa para Colombia y la región, especialmente en sectores que utilizan Microsoft SharePoint como plataforma colaborativa crítica, como entidades gubernamentales, financieras y de salud. Su explotación, sin necesidad de autenticación, expone a las organizaciones a accesos no autorizados, captura de información sensible y potenciales interrupciones operativas.

En un contexto donde muchas organizaciones aún enfrentan desafíos en la aplicación oportuna de parches, esta debilidad incrementa el riesgo de ciberataques dirigidos, afectando la confianza digital, la continuidad del negocio y la soberanía de la información en infraestructuras clave.

Soluciones y mitigaciones disponibles

- ❑ Instalar inmediatamente las actualizaciones de seguridad proporcionadas por Microsoft para SharePoint Server que corrigen esta vulnerabilidad crítica.
- ❑ Implementar reglas de detección en soluciones EDR/SIEM usando IOC conocidos (hashes, nombres de archivos como spinstall0.aspx, IP maliciosas, cadenas en logs de IIS, etc.) para identificar actividad anómala asociada a esta falla.
- ❑ Limitar el acceso a los servidores SharePoint desde redes externas o no confiables, especialmente si no son necesarios para operaciones remotas.
- ❑ Revisar los directorios de carga en SharePoint (_layouts, /_catalogs/masterpage/, etc.) en busca de archivos .aspx sospechosos o no autorizados.
- ❑ Configurar restricciones para evitar la carga de archivos ejecutables y asegurar que los servidores validen adecuadamente los tokens y datos de vista (__VIEWSTATE) antes de ejecutarlos.

Indicadores de Compromiso (IOC)

TIPO DE IOC	VALOR
md5	02b4571470d83163d103112f07f1c434
md5	9ed482741a24bba11df38b773a15d39f
md5	9b7c02c994c2e7df3cc2ebe77e81e9ad
md5	c4cbf79c7121e72888b56a670ac297e2
md5	d0bccf604f3721ec41f1142dda23f32f
md5	c738eb1fe0ebeffe75d22141e891e74f
md5	d2a77b0b23773c5ff93bb54f03060286
md5	2755a4c13d47dfc826ce700b961e78fe
md5	40e609840ef3f7fea94d53998ec9f97f
sha1	f5b60a8ead96703080e73a1f79c3e70ff44df271
sha1	7f21382d6f09cb2336255b9484013c756a7d9282
sha1	50baf689726b76850590c89cc2451c2ed0afe915
sha1	76746b48a78a3828b64924f4aedca2e4c49b6735
sha1	c06ffcd6b18b1dca51b58d07da1dc89605e31de3

TIPO DE IOC	VALOR
sha1	950aa10a81ba10b955c67be49af80e91190a9231
sha1	fe3a3042890c1f11361368aeb2cc12647a6fdae1
sha1	8fbab292edf3098da29a8c968679ab7c0f8ae918
sha1	141af6bcefdcf6b627425b5b2e02342c081e8d36
sha256	92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514
sha256	4a02a72aedc3356d8cb38f01f0e0b9f26ddc5ccb7c0f04a561337cf24aa84030
sha256	7baf220eb89f2a216fcb2d0e9aa021b2a10324f0641caf8b7a9088e4e45bec95
sha256	8d3d3f3a17d233bc8562765e61f7314ca7a08130ac0fb153ffd091612920b0f2
sha256	27c45b8ed7b8a7e5fff473b50c24028bd028a9fe8e25e5cea2bf5e676e531014
sha256	b336f936be13b3d01a8544ea3906193608022b40c28dd8f1f281e361c9b64e93
sha256	d50a7f142a53a8d2358137e74901e093e19047b66f42216163b91f26460d329b
sha256	1116231836ce7c8c64dd86027b458c3bf0ef176022beadfa01ba29591990aee6
sha256	3461da3a2ddcced4a00f87dcd7650af48f97998a3ac9ca649d7ef3b7332bd997
IP	96[.]9[.]125[.]147
IP	139[.]144[.]199[.]41
IP	89[.]46[.]223[.]88
IP	149[.]40[.]50[.]15
IP	154[.]223[.]19[.]106
IP	185.197.248[.]131
IP	131[.]226[.]2[.]6
IP	134.199.202[.]205
IP	188.130.206[.]168

FUENTES:

Microsoft Security Response Center (MSRC). Detalles sobre CVE-2025-53770, actores atribuidos, técnicas utilizadas, mitigar mediante parches, rotación de claves, habilitar AMSI y Defender.
https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770/

Informes internos de inteligencia de ColCERT y análisis técnico de fuentes corporativas internas (no divulgadas públicamente), que corroboran actividad adversaria activa, recopilación de IOC y validación de tácticas utilizadas por grupos cibercriminales, alineadas con la campaña ToolShell.