Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

EXPLOTACIÓN DE LA VULNERABILIDAD CVE-2025-53770 EN SHAREPOINT

21/ 07/ 2025

CONTENIDO

INTRODUCCIÓN

Recientemente se dio a conocer un problema de seguridad crítico que afecta a las versiones on-premises (locales) de Microsoft SharePoint Sever CVE-2025-53770. Es una vulnerabilidad Zero-day, esto quiere decir que estaba siendo explotada activamente antes de que Microsoft liberara un parche.

EXPLOTACIÓN DE LA VULNERABILIDAD CVE-2025-53770 EN SHAREPOINT

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_07_21_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	21/07/2025
Es día cero (0 day):	Si

RESUMEN

Recientemente se dio a conocer un problema de seguridad crítico que afecta a las versiones on-premises (locales) de Microsoft SharePoint Sever CVE-2025-53770. Es una vulnerabilidad Zero-day, esto quiere decir que estaba siendo explotada activamente antes de que Microsoft liberara un parche. Se le colocó una criticidad de CVSS: 9.8 siendo crítica.

Esta es una vulnerabilidad que permite la ejecución de código remoto, esto hace que un atacante no autenticado pueda ejecutar comandos arbitrarios en un servidor Sharepoint vulnerable.

Se le considera una deserialización de datos no confiables.

¿Cuáles son los afectados?

Esta vulnerabilidad afecta las versiones on-premises de Microsoft SharePoint Sever, incluyendo:

- SharePoint Server 2016
- SharePoint Server 2019
- SharePoint Subcription Edition

Importante

La versión de SharePoint Online (Microsoft 365) no se ve afectada por esta vulnerabilidad, ya que los servicios en la nube son gestionados y parcheados directamente por Microsoft.

CVE-2025-53770 es una variante de las vulnerabilidades anteriores (CVE-2025-49706 y CVE-2025-49704) que Microsoft ya había parcheado en su momento, esto nos deja ver lo insistentes que son los cibercriminales para encontrar nuevas formas de evadir los parches, explotando una debilidad similar.

¿Cómo funciona?

SharePoint como muchas otras aplicaciones necesitan procesar los datos que recibe, la parte importante viene cuando lo datos que se desean procesar vienen de una fuente no confiable y el proceso de deserialización no se maneja de forma correcta, aquí es cuando un atacante puede inyectar código malicioso en los datos, haciendo que el sistema lo ejecute.

La explotación a menudo utiliza una cadena de ataque conocida como (ToolShell). Los atacantes envían una solicitud HTTP POST maliciosa a un endpoint específico de SharePoint (/_layouts/15/ToolPane.aspx?DisplayMode=Edit) con un encabezado Referer falsificado a /_layouts/SignOut.aspx.

Esto engaña a SharePoint para que omita las verificaciones de autenticación y de resumen de formulario, permitiendo que el atacante sea tratado como un usuario autenticado sin realmente iniciar sesión.

Cuando ya está dentro, el cibercriminal trata de encontrar las llaves maestras de la oficina de SharePoint, es decir las Machine Keys. Estas permiten falsificar firmas en documentos o descifrar información secreta.

Tras robar las claves, los atacantes suelen desplegar “web shells” (pequeños archivos maliciosos, a menudo .aspx, como “spinstall0.aspx”. Estos webs shells actúan como puertas traseras que permiten al atacante ejecutar comandos, cargar o descargar archivos y controlar el servidor de forma remota a través de una interfaz web simple.

RECOMENDACIONES

- Microsoft todavía no ha lanzado parches se seguridad para cubrir esta vulnerabilidad, pero se recomienda ampliamente mantener actualizados sus sistemas.

- Reforzar las validaciones de identidad, por ejemplo, implementando o exigiendo autenticación multifactor (MFA) para todos los accesos administrativos y de usuario final.

- Implementa una solución de SIEM para detectar patrones de comportamiento sospechosos.

- Auditar los permisos y roles asignados a usuarios y servicios dentro de SharePoint. Asegúrate de que el principio de menor privilegio se aplique rigurosamente.

NOTICIA COMPLETA

https://devel.group/blog/explotacion-de-la-vulnerabilidad-cve-2025-53770-en-sharepoint/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group