La vulnerabilidad de día cero, identificada como CVE-2025-53770 (con una puntuación CVSS de 9.8), ha sido descrita como una variante de CVE-2025-49706 (CVSS 6.3), un fallo de suplantación en Microsoft SharePoint Server que fue corregido por la empresa tecnológica en el conjunto de actualizaciones de seguridad de julio de 2025.

"La deserialización de datos no confiables en instalaciones locales de Microsoft SharePoint Server permite a un atacante no autorizado ejecutar código a través de la red," señaló Microsoft en una advertencia publicada el 19 de julio de 2025.

La compañía también indicó que está *preparando y probando exhaustivamente una actualización integral* para abordar el problema. Agradeció a Viettel Cyber Security por el descubrimiento y reporte de la falla a través de la iniciativa Zero Day de Trend Micro (ZDI).

En una alerta separada emitida el sábado, Microsoft afirmó que tiene conocimiento de *ataques en curso dirigidos a clientes con instalaciones locales de SharePoint Server*, pero destacó que SharePoint Online, incluido en Microsoft 365, *no se ve afectado*.

Mientras no exista una solución oficial, Microsoft recomienda a los usuarios *habilitar la integración con la Interfaz de Análisis Antimalware (AMSI)* en SharePoint y *desplegar Microsoft Defender Antivirus en todos los servidores SharePoint*.

Cabe destacar que la integración con AMSI ya viene activada por defecto en la actualización de seguridad de septiembre de 2023 para SharePoint Server 2016/2019, así como en la actualización de características versión 23H2 de SharePoint Server Subscription Edition.

Para aquellos que no puedan habilitar AMSI, se aconseja *desconectar el servidor SharePoint de internet hasta que esté disponible un parche de seguridad*. Adicionalmente, se recomienda implementar Defender for Endpoint para detectar y bloquear actividad posterior a la explotación.

Esta revelación surge mientras Eye Security y la unidad 42 de Palo Alto Networks advirtieron sobre ataques que combinan CVE-2025-49706 y CVE-2025-49704 (CVSS 8.8), una

vulnerabilidad de inyección de código en SharePoint, para facilitar la ejecución de comandos arbitrarios en instancias vulnerables. Esta cadena de explotación ha sido denominada *ToolShell*.

Dado que CVE-2025-53770 es una *"variante" de CVE-2025-49706*, se sospecha que ambos vectores de ataque están relacionados.

Eye Security señaló que los ataques masivos identificados aprovechan CVE-2025-49706 para enviar una carga útil de ejecución remota mediante CVE-2025-49704. *"Creemos que agregar '_layouts/SignOut.aspx' como referencia HTTP convierte CVE-2025-49706 en CVE-2025-53770,"* explicó la firma.

Cabe mencionar que ZDI ha clasificado CVE-2025-49706 como una *vulnerabilidad de omisión de autenticación*, que se origina en la forma en que la aplicación procesa la cabecera HTTP Referer cuando se dirige al punto de conexión ToolPane («/_layouts/15/ToolPane.aspx»).

La actividad maliciosa consiste principalmente en *entregar cargas ASPX a través de PowerShell*, que luego se utilizan para robar la configuración *MachineKey* del servidor SharePoint, incluidas las claves *ValidationKey* y *DecryptionKey*, lo que permite mantener acceso persistente.

La empresa holandesa de ciberseguridad indicó que estas claves son fundamentales para generar cargas útiles válidas de *VIEWSTATE*, y que obtenerlas *convierte cualquier solicitud autenticada de SharePoint en una oportunidad de ejecución remota de código*.

"Aún estamos detectando oleadas masivas de explotación," declaró el CTO de Eye Security, Piet Kerkhofs. *"Esto tendrá un impacto enorme, ya que los atacantes se están moviendo lateralmente con gran rapidez mediante esta capacidad de ejecución remota."*

Hasta el momento, se han identificado más de 85 servidores SharePoint comprometidos con shells web maliciosas. Estos servidores pertenecen a 29 organizaciones distintas, incluidas empresas multinacionales y entidades gubernamentales.

Es importante señalar que Microsoft *aún no ha actualizado sus avisos* sobre CVE-2025-49706 y CVE-2025-49704 para reflejar la explotación activa. También se ha contactado a la compañía para obtener más detalles, y se actualizará la información en cuanto haya respuesta.