Nro. Alerta:	AL-2025-041	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	08-ago-2025	Actualización vulnerabilidad ToolShell- SharePoint	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Actualización Vulnerabilidad ToolShell-SharePoint
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Actualización vulnerabilidad ToolShell - SharePoint - figura referencial

Actualización vulnerabilidad ToolShell- SharePoint, CISA informa recibió archivos de webshells, DLL loader y key stealer, relacionados con las vulnerabilidades en Microsoft SharePoint Server.

III. INTRODUCCIÓN

Microsoft informa, que actores de amenazas han llevado a cabo una cadena de explotación para obtener acceso no autorizado a sus servidores de Sharepoint mediante CVE-2025-49706 (una vulnerabilidad de suplantación de red) y CVE-2025-49704 (una vulnerabilidad de ejecución remota de código - RCE), aunque no ha confirmado la explotación de CVE-2025-53771, la CISA considera que es probable, ya que puede combinarse con CVE-2025-53770 para eludir vulnerabilidades previamente divulgadas (CVE-2025-49704 y CVE-2025-49706).

IV. VECTOR DE ATAQUE

El análisis incluye 2 binarios .NET (DLL, bibliotecas de enlace dinámico) codificados en Base64 y 4 archivos ASPX (Active Server Page Extended) y 1 criptografía de key stealer.

Los archivos DLL decodificados están diseñados para recuperar configuraciones de **claves de máquina** (*machine key*) dentro de la configuración de una aplicación **ASP.NET** y agregar los valores obtenidos a los encabezados de respuesta **HTTP**.

- osvmhdfl.dll
- bjcloiyq.dll

Para el robo de claves criptográficos:

- stage3.txt

Usa un conjunto de WebShells son usados:

- Spinstall0.aspx, para recuperar y mostrar información de las claves de máquina de la configuración de una aplicación ASP.NET.
- Info3.aspx, contiene una instrucción de línea de comandos para ejecutar un comando de PowerShell, diseñado para decodificar en Base64 e instalar un webshell ASPX malicioso en el disco.
- Spinstallp.aspx y Spinstallb.aspx, se utilizan para ejecutar comandos en el servidor mediante PowerShell.

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 afectadas - Actualización vulnerabilidad ToolShell - SharePoint

VI. INDICADORES DE COMPROMISO

MD5	
osvmhdfl.dll	40e609840ef3f7fea94d53998ec9f97f
bjcloiyq.dll	0e36ecda6fc4b5661f9a181984a53bb5

MD5	
stage3.txt	921ac86b258fa9ea3da4c39462bad782
spinstall0.aspx	02b4571470d83163d103112f07f1c434
info3.aspx	1f5c8df6bd296ebf68acda951a004a5b
spinstallp.aspx	7768feda9d79ef6f87410c02e981f066
spinstallb.aspx	7d2f36f4cb82c75b83c210e655649b5d

Tabla 2.- MD5 - Actualización vulnerabilidad ToolShell - SharePoint

SHA1	
osvmhdfl.dll	141af6bcefdcf6b627425b5b2e02342c081e8d36
bjcloiyq.dll	3a438b239d8451b8e12e9cdd3c24d1240dd758c9
stage3.txt	b8662c8cc9e383b4a0ac980e0fd94941fe12c31d
spinstall0.aspx	f5b60a8ead96703080e73a1f79c3e70ff44df271
info3.aspx	d80722b335806cb74ee27af385abc6c9b018e133
spinstallp.aspx	1b8432fcda4c12b64cdf4918adf7880aecf054ec
spinstallb.aspx	37d1d1913d758f7d71020c08d4a7dae3efe83b68

Tabla 3.- SHA1 - Actualización vulnerabilidad ToolShell - SharePoint

SHA256	
osvmhdfl.dll	3461da3a2ddcced4a00f87dcd7650af48f97998a3ac9ca649d7ef3b7332bd997
bjcloiyq.dll	bee94b93c1796981a55d7bd27a32345a61304a88ed6cd70a5f7a402f1332df72
stage3.txt	60a37499f9b02c203af24c2dfd7fdb3834cea707c4c56b410a7e68376938c4b7
spinstall0.aspx	92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514
info3.aspx	9340bf7378234db5bca0dc5378bf764b6a24bb87a42b05fa21a996340608fbd7
spinstallp.aspx	d0c4d6a4be0a65f8ca89e828a3bc810572fff3b3978ff0552a8868c69f83d170
spinstallb.aspx	d9c4dd5a8317d1d83b5cc3482e95602f721d58e3ba624d131a9472f927d33b00

Tabla 4.- SHA256 - Actualización vulnerabilidad ToolShell - SharePoint

IPS
107.191.58.76
104.238.159.149
96.9.125.147
103.186.30.186
45.77.155.170
139.144.199.41
172.174.82.132
89.46.223.88
45.77.155.170
154.223.19.106
185.197.248.131
149.40.50.15

IPS
64.176.50.109
149.28.124.70
206.166.251.228
95.179.158.42
86.48.9.38
128.199.240.182
212.125.27.102
91.132.95.60
134.199.202.205
131.226.2.6
188.130.206.168

Tabla 5.- IP - Actualización vulnerabilidad ToolShell - SharePoint

VII. RECOMENDACIONES:

- Mantener actualizadas las firmas y motores del antivirus.
- Aplicar parches actualizados del sistema operativo.
- Desactivar los servicios de Compartir archivos e impresoras.
- Si son necesarios, usar contraseñas seguras o autenticación por Active Directory.
- Restringir los permisos de los usuarios para instalar y ejecutar aplicaciones no autorizadas.
- No agregar usuarios al grupo de administradores locales a menos que sea necesario.
  Aplicar una política de contraseñas robustas y realizar cambios periódicos.
- Tener precaución al abrir archivos adjuntos en correos, incluso si son esperados y el remitente parece conocido.
- Activar un firewall personal en las estaciones de trabajo, configurado para denegar solicitudes de conexión no solicitadas.
- Deshabilitar servicios innecesarios en servidores y equipos de la organización.
- Analizar y eliminar archivos adjuntos sospechosos; verificar que el tipo de archivo coincida con su extensión real (comparar extensión con el encabezado del archivo).
- Monitorear el historial de navegación de los usuarios y restringir el acceso a sitios de contenido riesgoso.
- Ser precavido al usar medios extraíbles (memorias USB, discos externos, CDs, etc.).
- Escanear todo software descargado de Internet antes de ejecutarlo.
- Mantenerse informado sobre las últimas amenazas y aplicar Listas de Control de Acceso (ACLs) adecuadas.

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:

CISA (2025). CISA Releases Malware Analysis Report Associated with Microsoft SharePoint Vulnerabilities. https://www.cisa.gov/news-events/alerts/2025/08/06/cisa-releases-malware-analysis-report-associated-microsoft-sharepoint-vulnerabilities

CISA (2025). Malware Analysis Report – Microsoft SharePoint Exploitation. https://www.cisa.gov/news-events/alerts/2025/08/06/cisa-releases-malware-analysis-report-associated-microsoft-sharepoint-vulnerabilities

CISA (2025). Malware Analysis Report: AR25-218A. https://www.cisa.gov/news-events/analysis-reports/ar25-218a