I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Ejecución Remota de Código (RCE)
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Vulnerabilidad Crítica de Ejecución Remota de Código (RCE) en Microsoft SharePoint (CVE-2026-45659) - figura referencial

Microsoft liberó una actualización de seguridad para corregir la vulnerabilidad de ejecución remota de código (RCE) CVE-2026-45659 en Microsoft SharePoint. La falla, clasificada como CWE-502 (Deserialización de Datos No Confiables), permite que un atacante autenticado ejecute código arbitrario de forma remota en el servidor afectado mediante el envío de datos especialmente manipulados. La explotación no requiere interacción de otros usuarios y puede realizarse con privilegios bajos sobre la plataforma SharePoint.

III. INTRODUCCIÓN

La vulnerabilidad CVE-2026-45659 es una falla de ejecución remota de código (RCE) que afecta a implementaciones de Microsoft SharePoint, que corresponde a la debilidad CWE-502 - Deserialización de Datos No Confiables, la cual se produce cuando la aplicación deserializa datos provenientes de una fuente no confiable sin realizar las validaciones adecuadas. Como resultado, un atacante autenticado puede suministrar

datos especialmente diseñados para que sean interpretados como objetos válidos durante el proceso de deserialización, provocando la ejecución de código arbitrario en el servidor afectado y comprometiendo la confidencialidad, integridad y disponibilidad del sistema.

Debido a que Microsoft SharePoint constituye una plataforma central para la colaboración empresarial y se integra estrechamente con servicios como Microsoft Active Directory, Microsoft 365, Microsoft OneDrive y Microsoft Power Platform, la explotación exitosa de esta vulnerabilidad podría permitir a un atacante acceder a documentos confidenciales, tokens de sesión, credenciales y cuentas de servicio. Asimismo, podría proporcionar visibilidad sobre la red interna de la organización, facilitar movimientos laterales y abrir oportunidades para comprometer entornos de Active Directory y otros sistemas corporativos interconectados.

IV. VECTOR DE ATAQUE

La vulnerabilidad CVE-2026-45659 tiene un vector de ataque tipo RED CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C con nivel de severidad 8.8 CRÍTICO.

Detalle del proceso de ataque:

1. **Acceso inicial**

Los atacantes obtienen acceso mediante:

- Credenciales robadas
- Acceso a la VPN
- Credenciales con privilegios limitados
- Cuentas de usuarios y contratistas comprometidas (mediante phishing)

2. **Entrega de payload**

El atacante implementa una payload especialmente diseñada en un componente vulnerable de SharePoint, lo que provoca que:

- La aplicación que permite ver los datos controlados por el atacante como si fueran ejecutables.
- Malware que se va a ejecutar

3. **Ejecución remota de código**

Una explotación exitosa puede permitir a los atacantes:

- Ejecutar comandos de PowerShell
- Implementar shells web
- Establecer mecanismos de persistencia
- Descargar malware adicional

4. **Post explotación**

Una vez dentro del servidor, el atacante puede:

- Robar documentos sensibles
- Credenciales de cosecha
- Muévete lateralmente a través de la red
- Acceda a los servicios de MS conectados
- Implementar ransomware

V. IMPACTO

Las siguientes versiones son vulnerables si no cuentan con las actualizaciones correspondientes:

- SharePoint Enterprise Server 2016 anterior a 16.0.5552.1002
- SharePoint Server 2019 anterior a 16.0.10417.20128
- SharePoint Server Subscription Edition anterior a 16.0.19725.20280

VI. INDICADORES DE COMPROMISO

Microsoft ha reconocido a un investigador llamado MEOW por descubrir y notificar la vulnerabilidad y no se revelo específicamente los IoCs, sin embargo, se sugiere observar los siguientes comportamientos:

Creación o modificación inesperada de archivos:

- Archivos .aspx no autorizados (posibles web shells).
- DLLs desconocidas en directorios de SharePoint o IIS.
- Scripts PowerShell (.ps1) creados fuera de procedimientos administrativos normales.

Tareas programadas o servicios nuevos no autorizados.

- C:\inetpub\wwwroot\
- Directorios de SharePoint bajo C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\
- Carpetas temporales de IIS o ASP.NET.

Eventos de creación de procesos (por ejemplo, Event ID 4688) donde el proceso padre sea w3wp.exe.

- Eventos de instalación de servicios (Event ID 7045).
- Creación de cuentas locales o modificaciones de grupos privilegiados.

VII. RECOMENDACIONES:

- Aplicar inmediatamente las actualizaciones de seguridad publicadas por Microsoft.
- Verificar que los servidores SharePoint expuestos a Internet se encuentren completamente actualizados.
- Revisar los registros de autenticación para detectar cuentas de bajo privilegio con actividad inusual.
- Monitorear procesos anómalos iniciados por SharePoint (PowerShell, cmd.exe, wscript, cscript, etc.).
- Buscar indicadores de compromiso y realizar una revisión forense si se sospecha explotación.
- Restringir el acceso administrativo y aplicar el principio de mínimo privilegio.

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:

MICROSOFT SECURITY RESPONSE CENTER (MSRC). (2026). *CVE-2026-45659*. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45659

CVE PROGRAM. (2026). *CVE-2026-45659*. https://www.cve.org/CVERecord?id=CVE-2026-45659

CSIRT TELCONET. (2026). *Vulnerabilidad de severidad alta en SharePoint Server permite ejecución remota de código (RCE).* https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-de-severidad-alta-en-sharepoint-server-permite-ejecucion-remota-de-codigo-rce/

THE HACKER NEWS. (2026). *Microsoft Patches SharePoint RCE Flaw.* https://thehackernews.com/2026/05/microsoft-patches-sharepoint-rce-flaw.html

SHARKSTRIKER. (2026). *CVE-2026-45659: Microsoft Patches a Major RCE Vulnerability in SharePoint.* https://sharkstriker.com/blog/cve-2026-45659-microsoft-patches-a-major-rce-vulnerability-in-sharepoint