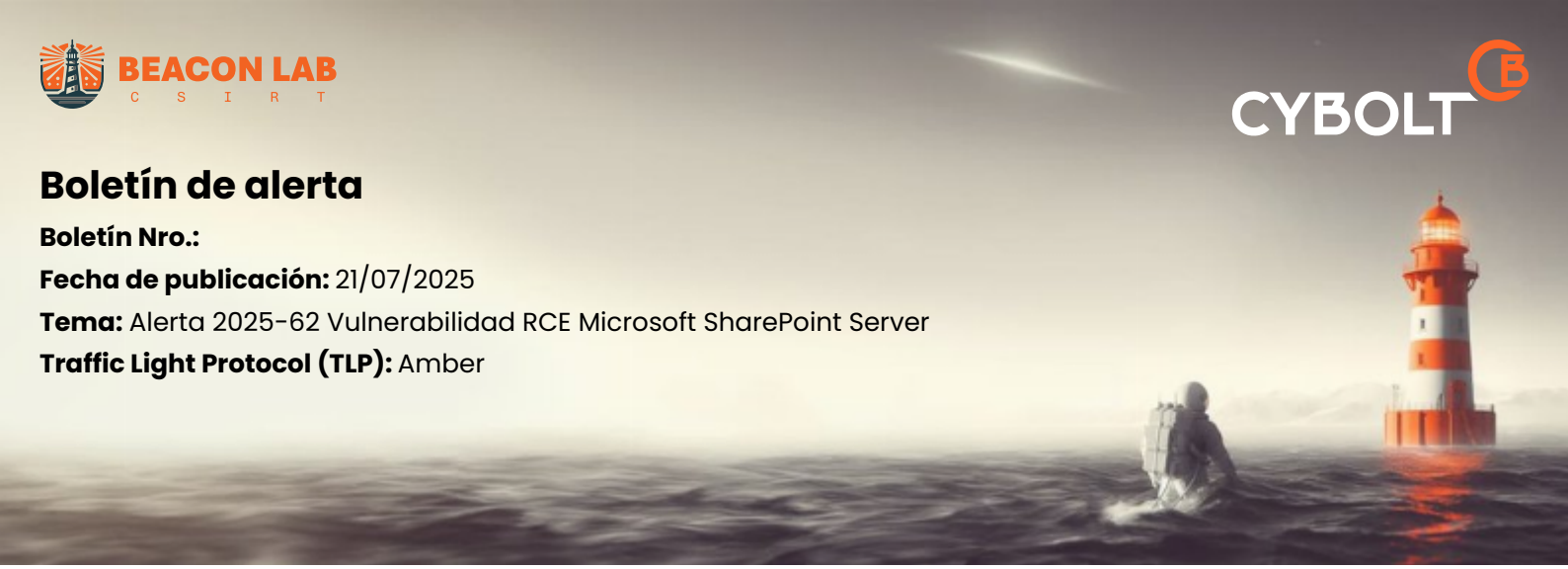

# Boletín de alerta

**Boletín Nro.:**
**Fecha de publicación:** 21/07/2025
**Tema:** Alerta 2025-62 Vulnerabilidad RCE Microsoft SharePoint Server
**Traffic Light Protocol (TLP):** Amber

## Producto(s) afectado(s):

- Microsoft SharePoint Enterprise Server 2016

## Descripción

Una deserialización de datos no confiables en Microsoft SharePoint Server local permite que un atacante no autorizado ejecute código a través de la red. Microsoft tiene conocimiento de la existencia de un exploit para CVE-2025-53770, con un score de 9.8.

Es una variante de la vulnerabilidad conocida como CVE-2025-49706. Su actividad de explotación está siendo reportada como «ToolShell» y proporciona acceso no autenticado a los sistemas permitiendo a actores maliciosos acceder completamente al contenido de SharePoint, incluyendo sistemas de archivos y configuraciones internas, y ejecutar código a través de la red.

Hasta el momento de la publicación de este boletín se tiene conocimiento de por lo menos 75 organizaciones donde se ha detectado la explotación exitosa.

## Solución:

Microsoft ha publicado actualizaciones de seguridad que protegen completamente a los clientes que usan SharePoint Subscription Edition y SharePoint 2019:

- Microsoft SharePoint Server Subscription Edition: **Microsoft SharePoint Server Subscription Edition (KB5002768).**
- Microsoft SharePoint Server 2019: **Microsoft SharePoint Server Subscription Edition (KB5002754).**

Adicionalmente para proteger el entorno local de SharePoint Server, se recomienda la integración de AMSI en SharePoint e implementación de Defender AV en todos los servidores de SharePoint. Esto impedirá que atacantes no autenticados aprovechen esta vulnerabilidad.

## Información adicional:

- https://thehackernews.com/2025/07/critical-microsoft-sharepoint-flaw.html
- https://www.cisa.gov/news-events/alerts/2025/07/20/microsoft-releases-guidance-exploitation-sharepoint-vulnerability-cve-2025-53770
- https://www.cve.org/CVERecord?id=CVE-2025-53770
- https://www.cisa.gov/news-events/alerts/2025/07/20/microsoft-releases-guidance-exploitation-sharepoint-vulnerability-cve-2025-53770
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/ejecucion-remota-de-codigo-en-sharepoint-server-de-microsoft?sstc=u88504nl570741