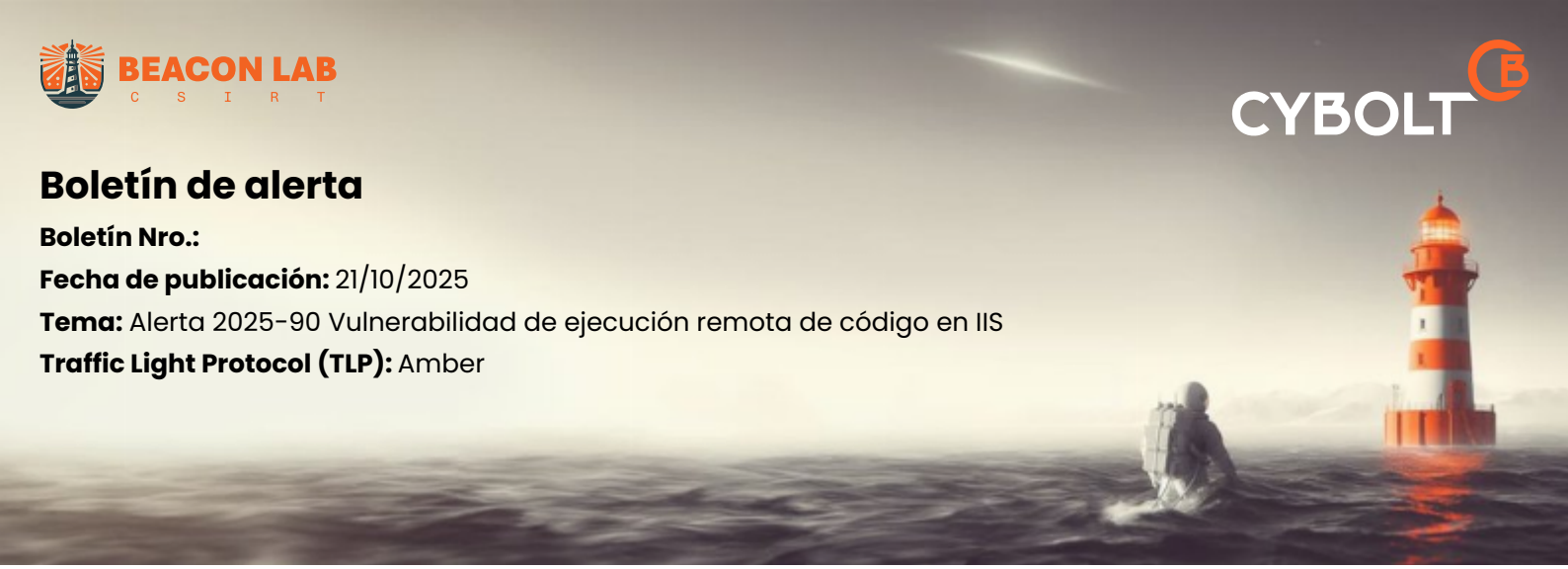

Boletín de alerta

Boletín Nro.:
Fecha de publicación: 21/10/2025
Tema: Alerta 2025-90 Vulnerabilidad de ejecución remota de código en IIS
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- **Internet Information Services (IIS)** — componente **Inbox COM Objects (Global Memory)** en sistemas Microsoft Windows. Afecta instalaciones de IIS en sistemas Windows/Windows Server.

Descripción

Recientemente, el equipo de Microsoft (MSRC) publicó y asignó la **CVE-2025-59282** como parte del boletín de seguridad de octubre de 2025. La vulnerabilidad se localiza en los *Inbox COM Objects* usados por IIS y componentes relacionados (objetos COM que manejan memoria/recursos globales). Microsoft la clasifica dentro del conjunto de correcciones liberadas en el Patch Tuesday de octubre 2025 con CVSS de 7.0.

Se trata de un manejo impropio de memoria concurrente en objetos COM de la pila de IIS. La explotación permite ejecución de código local (RCE) cuando se dan las condiciones necesarias de concurrencia y acceso a los recursos compartidos; el vector y el impacto han sido descritos por los analizadores como propensos a permitir que un atacante con posibilidad de ejecutar código local consiga elevar privilegios o ejecutar código en el contexto del servicio afectado, con impacto alto en confidencialidad, integridad y disponibilidad.

Aunque la vulnerabilidad permite RCE, la explotabilidad remota masiva depende de condiciones locales, por ejemplo acceso para provocar la condición de carrera, no obstante, Microsoft incluyó la corrección en su boletín y diversos centros de investigación recomiendan priorizar su mitigación en servidores que publiquen aplicaciones web o que tengan usuarios locales poco restringidos

Solución y recomendaciones:

Microsoft ha publicado un parche de seguridad en su actualización acumulativa de octubre de 2025 que corrige esta vulnerabilidad. Se recomienda lo siguiente:

- **Instalar el parche/actualización oficial de Microsoft** publicado en el boletín de seguridad de octubre de 2025 (Security Update Guide / MSRC). Esto es la solución primaria y obligatoria.

- **Inventariar servidores IIS** y priorizar actualizaciones en sistemas expuestos (servidores public web, app servers, entornos con acceso de múltiples usuarios locales). Use herramientas de gestión de parches (WSUS, SCCM/Intune, o su plataforma de MDM/patch management) para desplegar las actualizaciones de manera coordinada
- **Reducción de superficie**: si el componente *Inbox COM Objects* o funciones relacionadas no son necesarias, evaluar deshabilitar las características de IIS vinculadas o limitar el acceso local a cuentas no administradoras hasta aplicar parche. Varias notas de seguridad recomiendan revisar la lista de features instaladas y desactivar lo innecesario.

Información adicional:

- https://nvd.nist.gov/vuln/detail/CVE-2025-59282
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59282/
- https://blog.qualys.com/vulnerabilities-threat-research/2025/10/14/microsoft-patch-tuesday-october-2025-security-update-review