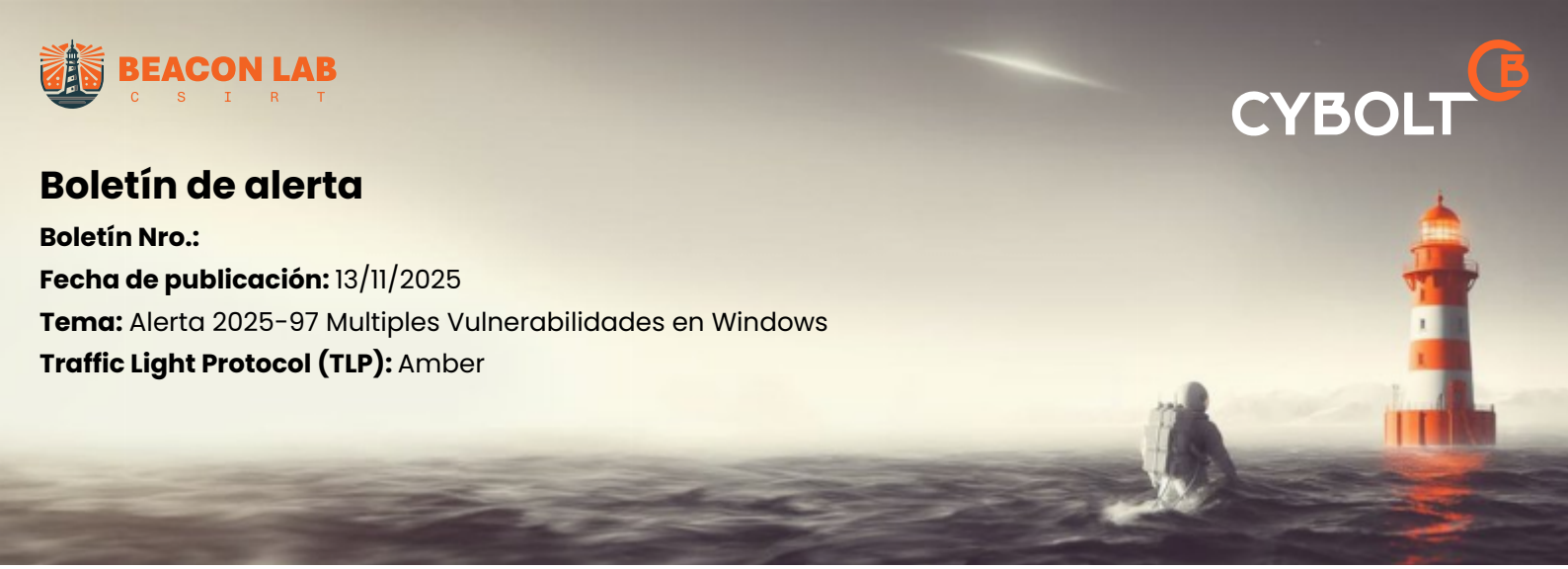

Boletín de alerta

Boletín Nro.:
Fecha de publicación: 13/11/2025
Tema: Alerta 2025-97 Multiples Vulnerabilidades en Windows
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Diversos productos de Microsoft entre ellos se destacan Windows 10 y 11.

Descripción

Se han reportado nuevas vulnerabilidades en productos Microsoft de diferencias criticidad, incluidas **cuatro críticas** y **una vulnerabilidad de día cero explotada activamente**. Las fallas impactan desde el núcleo de Windows hasta Office y componentes gráficos; muchas permiten **escalada de privilegios**, **ejecución remota de código (RCE)** o **divulgación de información**. Microsoft también publicó correcciones específicas (KB) para Windows 10 y Windows 11 en su actualización de Noviembre. Podemos destacar: **CVE-2025-62215 (CVSS: 7.0), CVE-2025-60724 (CVSS: 9.8), CVE-2025-62220 (CVSS: 8.8) y CVE-2025-60704 (CVSS: 7.5).**

A continuación se detallan las vulnerabilidades más importante:

CVE-2025-62215 — Vulnerabilidad de Día Cero en el Kernel (CVSS: 7.0)

Esta es una vulnerabilidad de **escalada de privilegios** de tipo día cero, lo que significa que ha sido observada en ataques reales. El fallo radica en una **condición de carrera** (*race condition*) dentro del kernel. Un atacante con acceso local y bajos privilegios puede manipular recursos compartidos para desencadenar una doble liberación de memoria, lo que resulta en la capacidad de sobrescribir la memoria del kernel. Esto permite la **ejecución de código con privilegios SYSTEM** (máximo nivel), siendo frecuentemente el paso final para comprometer completamente un sistema tras una intrusión inicial.

CVE-2025-60724 — Ejecución Remota de Código (RCE) en Componente Gráfico (CVSS: 9.8)

Clasificada con una puntuación CVSS crítica de 9.8, esta vulnerabilidad es un fallo de **Ejecución Remota de Código (RCE)**. Se debe a un **desbordamiento de *heap*** (*heap overflow*) dentro de un componente del subsistema gráfico. Si un sistema afectado procesa una entrada o archivo gráfico malicioso, esta condición puede permitir al atacante la **ejecución de código arbitrario de forma remota**, lo que representa un riesgo extremadamente alto.

CVE-2025-62220 — RCE en la Interfaz Gráfica de WSL (CVSS: 8.8)

Este es un fallo de **Ejecución Remota de Código (RCE)** que afecta específicamente a la interfaz gráfica de usuario (GUI) del **Windows Subsystem for Linux (WSL)**. Su impacto es significativo, ya que puede ser explotado a través de esta interfaz, permitiendo la **ejecución de código arbitrario** si el sistema no se actualiza con el parche correspondiente.

CVE-2025-60704 — Fallo de Escalada de Privilegios en Kerberos (CVSS: 7.5)

Esta vulnerabilidad afecta al protocolo **Kerberos** y se relaciona con los mecanismos de **delegación restringida** y el manejo de sumas de comprobación (*CheckSum*). El fallo posibilita la **escalada de privilegios** y la **suplantación de usuarios**. Bajo condiciones específicas—principalmente si el atacante ya tiene acceso a la red lógica entre la víctima y el recurso de destino—se puede suplantar la identidad de usuarios, lo que representa una amenaza potencial para **comprometer un dominio completo** de la red.

Solución:

Se recomienda aplicar las actualizaciones publicadas por Microsoft.

https://msrc.microsoft.com/update-guide

Información adicional:

- https://thehackernews.com/2025/11/microsoft-fixes-63-security-flaws.html
- https://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/actualizaciones-de-seguridad-de-microsoft-de-noviembre-de-2025
- https://msrc.microsoft.com/update-guide/