Boletín de alerta

Boletín Nro.:
Fecha de publicación: 15/10/2025
Tema: Alerta 2025-83 Multiples Vulnerabilidades en Windows
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Diversos productos de Microsoft

Descripción

Microsoft corrigió **180 vulnerabilidades** en octubre de 2025, incluyendo tres activamente explotadas (Días Cero). Las fallas más críticas son la **CVE-2025-59287 (WSUS)** con **CVSS 9.8** (RCE por deserialización), la **CVE-2025-55315 (ASP.NET)** con **CVSS 9.9** (*Request Smuggling*), y la **CVE-2025-49708 (VM Escape)** con **CVSS 9.9**. Estas vulnerabilidades permiten el control total del servidor, la evasión de seguridad y la ejecución de código en *hosts* desde máquinas virtuales, lo cual compromete la confidencialidad, integridad y disponibilidad de los entornos Windows.

Vulnerabilidades destacadas:

CVE-2025-24990 / CVE-2025-24052 (ltmdm64.sys — controlador Agere)

Los **CVE-2025-24990 con CVSS: 7,8 y CVE-2025-24052 con CVSS: 7,8** son una vulnerabilidad de corrupción de memoria en modo kernel que permite ejecución de código con privilegios de *ring 0*. Un atacante local puede manipular llamadas IOCTL al controlador y sobrescribir estructuras críticas del kernel. Esto permite instalar rootkits, desactivar mecanismos de seguridad (EDR/AV) y obtener control total del sistema. El riesgo es elevado incluso si el hardware no está presente, ya que el controlador vulnerable puede cargarse por defecto. Indicadores: llamadas IOCTL inusuales, BSOD tras carga del driver, o módulos kernel no firmados.

CVE-2025-59230 (RasMan — Remote Access Connection Manager)

La vulnerabilidad con el CVE**-2025-59230 con CVSS: 7,8** es una escalada de privilegios locales a **SYSTEM** por validación insuficiente en interfaces del servicio RasMan. Permite a un atacante con privilegios bajos ejecutar operaciones privilegiadas y obtener control total del host. Su explotación puede incluir desactivación de protecciones, persistencia elevada o movimiento lateral en redes Windows. Indicadores:

invocaciones no autorizadas a APIs de RasMan y creación de procesos con tokens elevados desde cuentas estándar.

CVE-2025-59287 (WSUS)

La vulnerabilidad con el **CVE-2025-59287 CVSS: 9.8,** es dentro de la vulnerabilidad se identifica unaejecución remota de código (RCE) mediante deserialización insegura en servidores WSUS. Un atacante puede enviar objetos manipulados que, al ser procesados, ejecutan código arbitrario con privilegios del servicio. Esto habilita la distribución de actualizaciones maliciosas o el control remoto del servidor. Indicadores: eventos de deserialización fallida, tráfico no esperado al puerto WSUS o ejecución de binarios no firmados por el proceso de actualización.

CVE-2025-55315 (ASP.NET)

vulnerabilidad con el **CVE-2025-55315 CVSS: 9.9,** es de *request smuggling* que permite contrabandear solicitudes HTTP dentro de otra petición legítima. Puede provocar evasión de controles de seguridad, manipulación de sesiones o ejecución de operaciones no autorizadas en aplicaciones ASP.NET autenticadas. Indicadores: solicitudes con delimitadores anómalos o múltiples peticiones dentro de una sola sesión autenticada.

CVE-2025-49708 (componentes gráficos / VM escape)

El **CVE-2025-49708 con CVSS: 9.9, es** unacorrupción de memoria en componentes gráficos del sistema que puede derivar en **escape de máquina virtual** o ejecución de código en el host desde una VM comprometida. Permite romper el aislamiento entre entornos virtualizados y acceder a datos de otras VMs. Indicadores: excepciones del hipervisor relacionadas con subsistemas gráficos y actividad inusual entre VM y host.

CVE-2025-59295 (URL parsing)

El **CVE-2025-59295 con CVSS: 8.8** es unacorrupción de memoria al procesar URLs malformadas. Una URL especialmente diseñada puede sobrescribir punteros o estructuras de ejecución y permitir **ejecución de código arbitrario** en el contexto del proceso afectado. Indicadores: crashes o excepciones de acceso a memoria en módulos que parsean URLs y peticiones HTTP con parámetros inusuales o excesivamente largos.

CVE-2025-58718 (Microsoft Remote Desktop Client — RCE)

El **CVE-2025-58718 con CVSS: 8.8,** la vulnerabilidad de **ejecución remota de código (RCE)** causada por el Cliente de Escritorio Remoto (RDP Client). Un servidor RDP malicioso puede aprovechar la gestión inadecuada de memoria para ejecutar código arbitrario en el contexto del usuario autenticado, tras

inducirlo a establecer conexión.

CVE-2025-47827 (IGEL OS <11 — Secure Boot Bypass)

El **CVE-2025-47827 con CVSS: 4.6,** es una validación defectuosa de la firma en imágenes del sistema que permite omitir el *Secure Boot*. Un atacante con acceso físico o control previo puede modificar la imagen raíz y ejecutar código antes del arranque del sistema. Impacta integridad del entorno y facilita instalación de rootkits persistentes. Indicadores: imágenes rootfs alteradas, arranques desde medios externos no autorizados o firmas inválidas aceptadas.

CVE-2025-2884 (TPM 2.0 — Implementación de referencia)

El **CVE-2025-2884 con CVSS: 5.3** es una lectura fuera de límites en la función CryptHmacSign, que puede provocar **divulgación de información sensible o denegación de servicio** del módulo TPM. Un atacante podría obtener datos intermedios relacionados con operaciones criptográficas o provocar fallos en procesos de arranque seguro. Indicadores: errores de firma, fallos del servicio TPM y logs con datos inesperados en operaciones de atestación o BitLocker.

Problemas de sincronización en Active Directory tras actualizaciones de Microsoft

Las actualizaciones de seguridad de septiembre y octubre de 2025 (KB5065426) provocan fallos en **Windows Server 2025**, afectando funciones críticas de **Active Directory Domain Services (AD DS)**, **Microsoft Entra Connect Sync** y **DirSync**. El error impide la sincronización completa de **grupos de seguridad con más de 10,000 miembros**, interrumpiendo procesos clave de autenticación, replicación y gestión de identidades en entornos híbridos.

Microsoft confirmó el problema el **14 de octubre de 2025** y desarrolla un parche correctivo. Como medida temporal, se recomienda modificar el registro del sistema para desactivar la función afectada, realizar copias de seguridad y probar las actualizaciones antes de implementarlas en entornos productivos.

https://learn.microsoft.com/en-us/windows/release-health/status-windows-server-2025#directory-synchronization-fails-for-ad-security-groups-exceeding-10-000-members

Solución:

Se recomienda aplicar las actualizaciones publicadas por Microsoft.

https://msrc.microsoft.com/update-guide/releaseNote/2025-Oct

Información adicional:

- https://thehackernews.com/2025/10/two-new-windows-zero-days-exploited-in.html
- https://www.bleepingcomputer.com/news/microsoft/microsoft-october-2025-patch-tuesday-fixes-6-zero-days-172-flaws/

- https://www.tenable.com/blog/microsofts-october-2025-patch-tuesday-addresses-167-cves-cve-2025-24990-cve-2025-59230