

Alerta Id	0049
Fecha del reporte	23/10/2025
Entidad	Todas las entidades del ecosistema digital
Título	Fallos críticos entorno de recuperación de Windows 11 tras la instalación de la actualización KB5066835 en Windows 11 (24H2 y 25H2) y Windows server 2025
Herramienta de detección	Análisis de fuentes oficiales (Microsoft, ADSLZone, www.techpowerup.com y foros especializados)
Activo involucrado	Microsoft Windows 11 (24H2 y 25H2) – Periféricos USB en entorno de recuperación (WinRE) y fallas en Windows Server 2025
Tipo de Alerta	Fallo de actualización
Nivel de riesgo	Alto

Objetivo

Informar a las entidades del ecosistema digital sobre la existencia de fallos críticos ocasionados por la actualización acumulativa KB5066835 de Windows 11 (versión 24H2 y 25H2), Microsoft confirmó que esta actualización interrumpe la funcionalidad del ratón y el teclado en el Entorno de recuperación de Windows (WinRE), dejándolos inoperativos. Como resultado, WinRE queda completamente inoperativo. WinRE es un kit de herramientas de solución de problemas integrado en Windows. Su objetivo es ayudar a los usuarios cuando su equipo presenta problemas de inicio o del sistema.



Descripción

La actualización **KB5066835**, publicada por Microsoft el 14 de octubre de 2025 como parte del ciclo de parches acumulativos de Windows 11, ha sido asociada no con fallos de seguridad que permita un ataque, sino un fallo funcional que impide la recuperación del sistema en caso de un error de arranque, bloqueando el acceso al Entorno de Recuperación de Windows (WinRE). Además, se han reportado fallos críticos en la autenticación de tarjetas inteligentes (Smart Cards) y en la replicación de Active Directory en servidores.

Microsoft ha reconocido oficialmente los problemas y ha comenzado a desplegar un parche de emergencia o actualización fuera de banda (OOB), la actualización es el KB5070762 la cual es acumulativa a la actualización pública el 14 de octubre del presente año, cabe resaltar que esta falla solamente se presenta en el entorno de WinRE, el teclado y el ratón USB siguen funcionando con normalidad en el sistema operativo Windows

Impacto

- Inoperatividad del Entorno de Recuperación (WinRE) (Riesgo CRÍTICO)

Tras instalar la actualización, si el usuario intenta acceder al Entorno de Recuperación (WinRE) (ya sea manualmente o por un fallo de arranque), el teclado y el ratón conectados por USB dejan de funcionar.

Este fallo es crítico, debido a que WinRE es la única herramienta integrada para solucionar problemas graves de arranque. Sin teclado ni ratón, el usuario no puede navegar por los menús de WinRE para:

- Desinstalar actualizaciones problemáticas.
- Usar la "Reparación de inicio".
- Restaurar el sistema a un punto anterior.
- Acceder al símbolo del sistema para reparaciones manuales.

El resultado es que, si el sistema operativo falla por cualquier motivo, el dispositivo queda efectivamente "brickeado" (inutilizable) y la única solución es una reinstalación completa del SO desde un medio externo, con el riesgo asociado de pérdida de datos.

Otras fallas reportadas.

- Fallo de Autenticación de Tarjeta Inteligente (Riesgo ALTO)

Se reportan problemas generalizados con la autenticación basada en certificados y tarjetas inteligentes (Smart Cards). Esto es un riesgo de seguridad operacional severo para entornos corporativos (empresariales y gubernamentales) que dependen de tarjetas inteligentes como método de autenticación multifactor (MFA) para iniciar sesión en estaciones de trabajo, firmar documentos o acceder a recursos de red.

- Fallo de Replicación de Active Directory (Riesgo CRÍTICO en Servidores)

En Windows Server 2025, la actualización causa un error de "incompatibilidad de esquema" (Error 8418) que interrumpe la replicación de Active Directory (AD). Este es un fallo catastrófico para una red empresarial. Impide que los controladores de dominio sincronicen la base de datos de seguridad central, lo que puede bloquear inicios de sesión, la aplicación de políticas de seguridad (GPOs) y comprometer la integridad de la infraestructura de identidad de la red.



- Ruptura de "Localhost"

La actualización impide las conexiones de red al "localhost" (127.0.0.1) bajo el protocolo HTTP/2, paralizando los entornos de prueba para desarrolladores.

Recomendaciones de mitigación

- Se recomienda a los usuarios de Windows 11 (24H2 y 25H2) que hayan instalado la KB5066835, o que estén experimentando estos problemas, buscar e instalar inmediatamente la actualización "fuera de banda" (Out-of-Band - OOB) de emergencia para solucionar estos problemas la cual es la actualización KB5070773.

Fuentes

- <https://support.microsoft.com/en-us/topic/october-20-2025-kb5070773-os-builds-26200-6901-and-26100-6901-out-of-band-0f533ed7-949a-4b89-8d0f-6ee751adfc4>
- <https://www.techpowerup.com/342032/windows-11-25h2-october-update-bug-renders-recovery-environment-unusable>
- <https://www.adslzone.net/noticias/windows/windows-11-lanza-actualizacion-emergencia-solucion-a-grave/>
- <https://microsofters.com/software/windows-11/kb5070773-parche-emergencia-arregla-winre-windows11-24h2-25h2/>

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas



telefónicas (+57) 316 893 1490 - 318 155 3570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

