Boletín de alerta

Boletín Nro.: 89
Fecha de publicación: 20/10/2025
Tema: Alerta 2025-89 Vulnerabilidad crítica activamente explotada en Windows Remote Access Connection Manager
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

La vulnerabilidad afecta componentes de los siguientes sistemas de Microsoft:

- Microsoft Windows (Windows 10, Windows 11)
- Microsoft Windows Server (ediciones Server 2008 R2, Server 2012, Server 2016, Server 2019, Server 2022, Server 2025)
- Específicamente al servicio Remote Access Connection Manager (RasMan) utilizado por Windows para gestionar conexiones de acceso remoto (dial-up y VPN)

Descripción

Recientemente, el equipo de respuesta de seguridad de Microsoft Corporation identificó una vulnerabilidad (**CVE-2025-59230**) de elevación de privilegios en su componente Remote Access Connection Manager (RasMan), que gestiona las conexiones de acceso remoto y redes privadas virtuales (VPN) en los sistemas Windows y que está siendo **activamente explotada**. Esta falla ha sido registrada con un CVSS v3.1 de **7.8**. Esta vulnerabilidad permite a un atacante con una cuenta válida en el sistema local con muy bajos privilegios escalar sus privilegios hasta el nivel del sistema (SYSTEM) sin interacción del usuario y con una complejidad de ataque relativamente baja.

La falla radica en que el servicio RasMan no valida correctamente los tokens de seguridad o los permisos al ejecutar ciertas operaciones que deberían estar restringidas, lo que permite que un usuario autorizado pero limitado manipule la lógica del servicio para ejecutar código con privilegios elevados. La explotación de esta falla permite al atacante obtener control completo del sistema, pudiendo leer, modificar o destruir datos confidenciales, instalar programas, cambiar configuraciones, o incluso persistir a nivel de kernel o sistema.

Solución:

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

- Aplicar **inmediatamente** las actualizaciones de seguridad de Microsoft correspondientes a octubre de 2025 para todos los sistemas afectados (clientes y servidores).
- Verificar que el servicio Remote Access Connection Manager (RasMan) esté actualizado y que la build del sistema sea posterior a la corregida para su versión específica de Windows.
- En entornos donde el parche no puede aplicarse de inmediato, considerar las siguientes medidas provisionales:
    - Monitorear eventos de elevación de privilegios y cambios en cuentas del sistema o en el servicio RasMan.
    - Limitar los accesos de usuarios no administrativos al equipo y auditar las cuentas con privilegios bajos que podrían intentar manipular servicios.
    - Aplicar el principio de mínimo privilegio: los usuarios no administrativos no deberían tener acceso a funciones de sistema crítico innecesarias.
    - Evaluar el aislamiento de sistemas críticos para que no ejecuten usuarios con privilegios que puedan escalar.

Información adicional:

- https://nvd.nist.gov/vuln/detail/CVE-2025-59230
- https://socprime.com/blog/cve-2025-59230-and-2025-24990-vulnerabilities/
- https://www.cisa.gov/news-events/alerts/2025/10/14/cisa-adds-five-known-exploited-vulnerabilities-catalog