Boletín de alerta

Boletín Nro.:
Fecha de publicación: 21/10/2025
Tema: Alerta 2025-91 Vulnerabilidad crítica en Windows SMB
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- **Microsoft Windows — SMB Client:** *versiones de cliente y servidor de Windows afectadas (Windows 10, Windows 11 y múltiples versiones de Windows Server; incluye ediciones hasta las ramas publicadas en 2024/2025).*

Descripción

Se ha reportaro una vulnerabilidad de control de acceso en el cliente SMB de Microsoft. La vulnerabilidad permite a un atacante con capacidad de autenticarse forzar una conexión SMB maliciosa que derive en escalamiento de privilegios a nivel SYSTEM en la máquina víctima. La CVE-2025-33073 ha sido calificada con **CVSS alto** de **8.8.**

El componente afectado es el cliente/implementación SMB usado para compartir archivos y autenticación entre hosts en entornos Windows.

La vulnerabilidad que permite elevación de privilegios por red cuando se explota correctamente. El vector de explotación descrito consiste en inducir a la víctima a autenticarse contra un servidor SMB controlado por el atacante (por ejemplo mediante técnicas de coerción de conexión, LLMNR/NBT-NS poisoning, o manipulación de resolución), y aprovechar la falta/incorrecta aplicación de controles en el protocolo para comprometer la sesión y ejecutar acciones con privilegios elevados.

Desde la publicación del parche en junio 2025 y la documentación técnica posterior, se han hecho análisis públicos, PoC y guías de detección que describen cómo la vulnerabilidad esquiva ciertas mitigaciones de NTLM-reflection y depende, en parte, de configuraciones como **SMB signing** no forzada o habilitada de forma débil en el entorno objetivo. Esto implica que entornos donde SMB signing no esté exigido son particularmente vulnerables. Además, se han publicado PoC experimentales que muestran métodos de explotación tanto en LAN como con técnicas de coacción de conexión a distancia.

Recomendaciones:

Configuraciones de mitigación mientras se planifica la aplicación del parchea:

- Forzar SMB Signing (require signing) en servidores y clientes cuando sea posible. Sistemas que obliguen SMB signing reducen la superficie de explotación.
- Restringir/filtrar tráfico SMB: bloquear SMB (TCP 445) a destinos externos, y limitar la exposición del servicio SMB sólo a redes internas de confianza mediante firewall/ACLs.
- Monitorización y detección: detectar conexiones SMB inusuales, coerción de autenticación (conexiones salientes que inician sesión NTLM/SMB hacia destinos no habituales) y alertar sobre resoluciones LLMNR/NBT-NS anómalas. Se han publicado scripts/IoCs y PoC que ayudan a crear reglas de detección.
- Aplicar medidas de hardening: políticas de bloqueo de NTLM v1, migrar a Kerberos donde sea posible, y revisar registros de eventos de seguridad para rastros de autenticaciones SMB anómalas.

Solución:

Aplicar el parche oficial de Microsoft inmediatamente: Microsoft publicó la actualización de seguridad para CVE-2025-33073; aplique los boletines y parches correspondientes en todos los endpoints y servidores.

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-33073

CISA: acción urgente — CISA ha añadido CVE-2025-33073 a su Known Exploited Vulnerabilities catalog, lo que eleva la prioridad de remediación en organizaciones del sector público y requiere atención inmediata según BOD aplicables. Priorice la remediación en activos críticos.

En entornos no parcheables inmediatamente: considere retirar temporalmente la funcionalidad SMB desde accesos expuestos a zonas no seguras, aislar hosts críticos, y realizar inventario priorizado para parcheo inmediato.

Información adicional:

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-33073
- https://www.cisa.gov/news-events/alerts/2025/10/20/cisa-adds-five-known-exploited-vulnerabilities-catalog
- https://www.synacktiv.com/en/publications/ntlm-reflection-is-dead-long-live-ntlm-reflection-an-in-depth-analysis-of-cve-2025