Boletín de alerta

Boletín Nro.:
Fecha de publicación: 13/08/2025
Tema: Alerta 2025-69 Multiples Vulnerabilidades en Windows
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Diversos productos de Miscrosoft

Descripción

El Martes de Parches de agosto de 2025 de Microsoft, incluyo actualizaciones de seguridad para 107 vulnerabilidades, incluyendo una vulnerabilidad de día cero en Windows Kerberos, divulgada públicamente.

Este Martes de Parches también corrige trece vulnerabilidades «críticas»: nueve de ellas son de ejecución remota de código, tres de divulgación de información y una de elevación de privilegios.

A continuación, se muestra el número de errores en cada categoría de vulnerabilidad:

- 44 Vulnerabilidades de Elevación de Privilegios
- 35 Vulnerabilidades de Ejecución Remota de Código
- 18 Vulnerabilidades de Divulgación de Información
- 4 Vulnerabilidades de Denegación de Servicio
- 9 Vulnerabilidades de Suplantación de Identidad

La vulnerabilidad de día cero divulgada públicamente es:

- **CVE-2025-53779**: Vulnerabilidad de Elevación de Privilegios en Windows Kerberos

Microsoft ya ha corregido la vulnerabilidad en Windows Kerberos que permite a un atacante autenticado obtener privilegios de administrador de dominio, mediante un path transversal en Windows Kerberos.

Microsoft afirma que un atacante necesitaría tener acceso elevado a los siguientes atributos de la dMSA para explotar la vulnerabilidad:

- **msds-groupMSAMembership**: Este atributo permite al usuario utilizar la dMSA.

- **msds-ManagedAccountPrecededByLink**: El atacante necesita acceso de escritura a este atributo, lo que le permite especificar un usuario en cuyo nombre puede actuar la dMSA.

Otra falla crítica, identificada como **CVE-2025-53783**, podría permitir que un atacante no autorizado lea, escriba e incluso elimine mensajes y datos de usuario mediante la ejecución de código a través de una red. Un atacante podría explotar esta falla para sobrescribir datos críticos o ejecutar código malicioso dentro de la aplicación Teams.

Microsoft afirma que una explotación funcional de esta falla podría tener consecuencias significativas para la confidencialidad, integridad y accesibilidad de los datos de un usuario, lo que permitiría al atacante obtener derechos de lectura, escritura y eliminación de datos.

La vulnerabilidad es un desbordamiento de búfer de montón, un tipo de corrupción de memoria en el que una aplicación puede verse obligada a almacenar datos más allá del espacio de memoria asignado.

Mitigación:

Se recomienda aplicar las actualizaciones publicadas por Microsoft.

Información adicional:

- https://www.bleepingcomputer.com/news/microsoft/microsoft-august-2025-patch-tuesday-fixes-one-zero-day-107-flaws/
- https://www.akamai.com/blog/security-research/abusing-dmsa-for-privilege-escalation-in-active-directory'
- https://cybersecuritynews.com/microsoft-teams-rce-vulnerability/