Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

PATCH TUESDAY DE JULIO 2025 MICROSOFT CORRIGE 137 VULNERABILIDADES

09/ 07 / 2025

CONTENIDO

INTRODUCCIÓN

El gigante tecnológico Microsoft ha lanzado una serie de actualizaciones de seguridad que corrigen múltiples vulnerabilidades, para ser exactos un total de137 vulnerabilidades incluyendo un Zero-day de divulgación pública.

PATCH TUESDAY DE JULIO 2025 MICROSOFT CORRIGE 137 VULNERABILIDADES

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_07_09_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	09/07/2025
Es día cero (0 day):	Si

RESUMEN

El gigante tecnológico Microsoft ha lanzado una serie de actualizaciones de seguridad que corrigen múltiples vulnerabilidades, para ser exactos un total de137 vulnerabilidades incluyendo un Zero-day de divulgación pública, esta afecta al producto de Microsoft SQL Server.

Categorización de vulnerabilidades

- 53 elevación de vulnerabilidades de escalación privilegios
- 8 vulnerabilidades de omisión de funciones de seguridad
- 41 vulnerabilidades de ejecución remota de código
- 18 vulnerabilidades de divulgación de información
- 6 vulnerabilidades de denegación de servicio
- 4 vulnerabilidades de suplantación de identidad
- 7 vulnerabilidades (4 de Mariner y 3 de Microsoft Edge) solucionadas a principios de este mes

Zero-day en Microsoft SQL Server

Esta vulnerabilidad está basada en la fuga de información, esto puede permitir que un atacante remoto sin autenticación pueda acceder a datos en memoria no inicializada.

Se le dio un puntaje de CVVS: 7.5 lo cual la categoriza como una vulnerabilidad alta, aunque Microsoft mencionó que puede ser una explotación poco probable, pero el código publicado podría cambiar eso.

¿Cómo actúa?

La falta de verificación correcta de datos de entrada en SQL server puede hacer que el componente del sistema devuelva contenido de memoria residual, exponiendo credenciales o información sensible.

¿Cuál es la solución?

Se recomienda hacer la actualización de SQL Server y el OLE DB Driver a las versiones 18 o 19, siempre es necesario revisar la compatibilidad antes de hacerlo.

Vulnerabilidades criticas

Además de la vulnerabilidad Zero-day, también se corrigieron 14 vulnerabilidades catalogadas como críticas. 10 de estas tienen que ver con RCE.

RCE en Microsoft Office: Se solucionaron problemas que permiten ejecución remota al abrir documentos maliciosos, incluso simplemente mediante la vista previa.

RCE en SharePoint: Vulnerabilidad (CVE-2025-49704) que permite atacantes con cuenta en el sistema provocar ejecución de código remoto.

A continuación, se muestra una tabla con las 14 vulnerabilidades más destacadas:

Etiqueta	CVE ID	Título CVE	Descripción de la vulnerabilidad	Severidad
Cola de datos AMD L1	CVE-2025-36357	AMD: CVE-2025-36357	Ataque transitorio en cola de datos L1.	Crítico
Cola de la tienda AMD	CVE-2025-36350	AMD: CVE-2024-36350	Ataque de programador transitorio en la cola de la tienda.	Crítico
Microsoft Office	CVE-2025-49697	Vulnerabilidad de ejecución remota de código de Microsoft Office	Permite la ejecución remota de código en Microsoft Office.	Crítico
Microsoft Office	CVE-2025-49695	Vulnerabilidad de ejecución remota de código de Microsoft Office	Permite la ejecución remota de código en Microsoft Office.	Crítico
Microsoft Office	CVE-2025-49696	Vulnerabilidad de ejecución remota de código de Microsoft Office	Permite la ejecución remota de código en Microsoft Office.	Crítico
Microsoft Office	CVE-2025-49702	Vulnerabilidad de ejecución remota de código de Microsoft Office	Permite la ejecución remota de código en Microsoft Office.	Crítico
Microsoft Office SharePoint	CVE-2025-49704	Vulnerabilidad de ejecución remota de código de Microsoft Office SharePoint	Permite la ejecución remota de código en Microsoft Office SharePoint.	Crítico
Microsoft Office Word	CVE-2025-49703	Vulnerabilidad de ejecución remota de	Permite la ejecución remota	Crítico

		código de Microsoft Word	de código en Microsoft Word.	
Microsoft Office Word	CVE-2025-49698	Vulnerabilidad de ejecución remota de código de Microsoft Word	Permite la ejecución remota de código en Microsoft Word.	Crítico
Rol: Windows Hyper-V	CVE-2025-48822	Vulnerabilidad de ejecución remota de código de asignación discreta de dispositivos (DDA) de Windows Hyper-V	Permite la ejecución remota de código a través de la asignación discreta de dispositivos en Windows Hyper-V.	Crítico
Servidor SQL	CVE-2025-49717	Vulnerabilidad de ejecución remota de código de Microsoft SQL Server	Permite la ejecución remota de código en Microsoft SQL Server.	Crítico
Componente de imágenes de Windows	CVE-2025-47980	Vulnerabilidad de divulgación de información de componentes de imágenes de Windows	Divulgación de información sensible en los componentes de imágenes de Windows.	Crítico
Servicio de proxy KDC de Windows (KPSSVC)	CVE-2025-49735	Vulnerabilidad de ejecución remota de código del servicio de proxy KDC de Windows (KPSSVC)	Permite la ejecución remota de código en el servicio de proxy KDC de Windows.	Crítico
Negociación extendida de Windows SPNEGO	CVE-2025-47981	Vulnerabilidad de ejecución remota de código del mecanismo de seguridad SPNEGO Extended Negotiation (NEGOTEX)	Permite la ejecución remota de código en el mecanismo de seguridad SPNEGO Extended Negotiation.	Crítico

Elevación de privilegios y bypass de seguridad

Se corrigieron 53 vulnerabilidades relacionadas a la elevación de privilegios (EoP), Muchas llegando a nivel SYSTEM si se ejecuta código malicioso con autenticación local.

También se encontraron 8 bypass de características de seguridad, varios en BitLocker, permitiendo así eludir cifrado, Smart creen y el componente de licencias de escritorio remoto.

Fugas de información

Durante el Patch Tuesday de julio 2025, Microsoft solucionó 18 vulnerabilidades de divulgación de información, muchas de las cuales podrían ser aprovechadas para filtrar datos sensibles desde la memoria del sistema operativo o de aplicaciones críticas.

Además del zero-day CVE-2025-49719, se corrigieron otras vulnerabilidades que afectan al procesamiento de datos en memoria por parte de SQL Server. Estas pueden exponer fragmentos de memoria no inicializada, especialmente al ejecutar ciertas consultas o procedimientos almacenados con entradas manipuladas.

Una vulnerabilidad en el Graphics Device Interface (GDI), el motor gráfico de Windows permitía que aplicaciones con bajo nivel de privilegio accedieran a contenido residual en memoria gráfica o de texto renderizado.

Windows Strorage Managament Provider, este componente de Windows se encarga de interactuar con discos duros, volúmenes y configuraciones de almacenamiento. La vulnerabilidad permitía el acceso a estructuras internas que no estaban correctamente limpiadas tras ciertas operaciones.

¿Por qué son importantes las fugas de información?

Aunque estas vulnerabilidades no ejecutan código ni escalan privilegios directamente, son valiosas para atacantes que buscan:

- Reconocimiento previo al ataque (identificar configuraciones internas).
- Recopilación de información confidencial sin levantar alertas.
- Soporte a exploits más complejos que combinan fuga de datos + RCE o EoP.

Por tanto, es crítico tratarlas con la misma seriedad que otras vulnerabilidades de mayor puntuación en CVSS, especialmente en entornos empresariales o compartidos.

Otras vulnerabilidades importantes

Se encontraron 6 fallos relacionados a denegación de servicios (DoS) estos pueden hacer que componentes de Windows de bloqueen mediante red.

Se detectaron 4 spoofing Uno en SQL Server permitía suplantar credenciales en Pwn2Own, otro en WebAuthn/Escritorio remoto, SMB y recursos de red.

Se encontró Tampering un fallo en Windows StateRepository API Server que permite a aplicaciones enjauladas eliminar archivos del sistema.

RECOMENDACIONES

- Actualiza SQL Server y/o el controlador OLE DB a la última versión disponible.
- Aplica parches de seguridad para Office, SharePoint y otros productos afectados.
- Bloquea archivos sospechosos adjuntos en correos (por ejemplo, .docx, .xlsm).
- Instala todos los parches que corrigen EoP, especialmente en sistemas compartidos.
- Utiliza el principio de menor privilegio (Least Privilege) para todos los usuarios.
- Verifica que BitLocker esté correctamente configurado y activo después del parche.
- Ejecuta herramientas de escaneo de memoria y revisa integridad de datos.

NOTICIA COMPLETA

https://devel.group/blog/patch-tuesday-de-julio-2025-microsoft-corrige-137-vulnerabilidades/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group