Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

MICROSOFT CORRIGE 81 VULNERABILIDADES EN EL PATCH TUESDAY, INCLUYENDO DOS ZERO-DAYS

10/ 09/2025

CONTENIDO

INTRODUCCIÓN

Microsoft ha lanzado su parche de seguridad mensual para septiembre de 2025, corrigiendo 81 vulnerabilidades que afectan a múltiples productos, como Windows, Office, SharePoint, Hyper-V y componentes de red. Lo más preocupante es que dos de las vulnerabilidades, catalogadas como zero-days, ya habían sido reveladas y estaban siendo explotadas públicamente antes de que existiera una solución.

MICROSOFT CORRIGE 81 VULNERABILIDADES EN EL PATCH TUESDAY, INCLUYENDO DOS ZERO-DAYS

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

ID de alerta:	DSOC-CERT_2025_09_10_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	10/09/2025
Es día cero (0 day):	Si

RESUMEN

Microsoft ha lanzado su boletín de parches de seguridad mensual para septiembre de 2025, corrigiendo 81 vulnerabilidades que afectan a múltiples productos, como Windows, Office, SharePoint, Hyper-V y componentes de red. Lo más preocupante es que dos de las vulnerabilidades, catalogadas como zero-day, ya habían sido reveladas y estaban siendo explotadas públicamente antes de que existiera una solución.

Aunque el número total de fallos es menor que en meses anteriores, la gravedad de estos hace que esta actualización sea una prioridad para los administradores y equipos de seguridad.

Desglose de vulnerabilidades

El paquete de parches incluye correcciones para los siguientes tipos de vulnerabilidades:

- 38 de elevación de privilegios (EoP)
- 22 de ejecución remota de código (RCE)
- 14 de divulgación de información
- 4 denegación de servicio (DoS)
- 2 de omisión de seguridad
- 1 de suplantación de identidad

Según los investigadores, al menos 8 de estas vulnerabilidades se clasifican como críticas, mientras que el resto son considerados importantes.

Días cero corregidos

Los dos zero-days que ya estaban siendo explotados son:

- CVE-2025-55234 – Elevación de privilegios para SMB de Windows: Con un CVSS de 8.8, este fallo permite a los atacantes lanzar ataques de retransmisión en SMB, comprometiendo entornos que no tienen activados mecanismos de seguridad como SMB Signing o Extended Protection for Authentication (EPA). Esto representa un alto riesgo para las redes corporativas que usan Active Directory.
- CVE-2024-21907 – Newtonsoft.Json (BlogEngine.NET): Esta vulnerabilidad permite la ejecución remota de código a través de la manipulación de objetos JSON. Aunque su alcance es más limitado, sigue siendo relevante para entornos web que utilizan este framework.

Otras vulnerabilidades de alto riesgo

- CVE-2025-54918 : Una falla de elevación de privilegios en Windows NTLM que permite a un atacante con acceso a la red elevar sus permisos hasta el nivel de sistema. Tiene una puntuación CVSS de 8.8.
- CVE-2025-55226 : Una vulnerabilidad de ejecución de código remoto (RCE) en el kernel de gráficos de Windows. Requiere acceso local y es considerado de riesgo medio, con un CVSS de 6.7.

- CVE-2025-55228 : Una vulnerabilidad de ejecución de código remoto (RCE) en el componente Windows Win32K. Un atacante con privilegios bajos puede ejecutar código de forma local, con un CVSS de 7.8.
- CVE-2025-55236 : Una vulnerabilidad de ejecución de código remoto (RCE) en el kernel de gráficos de Windows. Un atacante local con pocos privilegios puede explotarla para ejecutar código. Su CVSS es de 7.3.
- CVE-2025-53799 : Una falla de divulgación de información en el Windows Imaging Component. Puede permitir que un atacante local revele información sensible. Tiene un CVSS de 5.5.
- CVE-2025-53800 : Una vulnerabilidad de elevación de privilegios (EoP) en el componente de gráficos de Windows que permite a un atacante obtener acceso local a permisos más altos. Su CVSS es de 7.8.
- CVE-2025-54910 : Una vulnerabilidad de ejecución de código remoto (RCE) en Microsoft Office que permite la ejecución de código a través de un desbordamiento de búfer sin interacción del usuario. Su CVSS es de 8.4.
- CVE-2025-55224 : Una vulnerabilidad de ejecución de código remoto (RCE) en el Windows Win32K – GRFX que se explota de forma local. Su CVSS es de 7.8.

Contexto más amplio

Este mes se confirma una tendencia: las vulnerabilidades de elevación de privilegios superan en número a las de ejecución remota de código. Esto significa que, aunque muchos requieren acceso previo al sistema, pueden ser el eslabón final para un compromiso total en cadenas de ataque combinados.
Si deseas más información, sobre las 81 vulnerabilidades pueden visualizarlo aquí.

RECOMENDACIONES

- Aplique los parches de inmediato en Windows 10, 11 y Windows Server.
- Habilita SMB Signing y EPA para mitigar ataques de retransmisión.
- Deshabilita las macros y la vista previa automática en Office/Outlook.
- Refuerza la seguridad en SharePoint y Hyper-V: revisa los permisos, la autenticación y la segmentación de red.
- Monitorea de forma proactiva con EDR/XDR para detectar intentos de explotación.

NOTICIA COMPLETA

https://devel.group/blog/microsoft-corrige-81-vulnerabilidades-en-el-patch-tuesday-incluyendo-dos-zero-days-criticos/

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