Alerta ID:	0068
Fecha del reporte:	10/12/2025
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades en Patch Tuesday de Microsoft – diciembre 2025
Herramienta de detección	Análisis de fuentes oficiales (Microsoft, Tenable, etc)
Activo involucrado:	Sistemas operativos Microsoft Windows, plataformas en la nube y servicios de azure, SQL Server, Microsoft Office, herramientas de desarrollo, entre otras herramientas.
Tipo de alerta:	Gestión de vulnerabilidades
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del ecosistema digital sobre las vulnerabilidades abordadas en el Patch Tuesday de Microsoft de diciembre de 2025, concientizando sobre los riesgos de explotación, facilitando la identificación de activos y versiones afectados, promoviendo la aplicación oportuna de parches y medidas de mitigación, y fortaleciendo la capacidad de respuesta ante incidentes de seguridad.

Descripción:

El 09 de 2025, Microsoft publicó su paquete mensual de actualizaciones de seguridad, abordando 57 vulnerabilidades incluyendo Windows, Office, SharePoint, Microsoft Edge, Azure, SQL Server, Hyper-V y más.

De las 57 vulnerabilidades reportadas por Microsoft se catalogaron 3 de nivel “criticas” y 54 importantes.

Adicionalmente se incluye 3 vulnerabilidades de tipo zero-day (1 bajo explotación activa, 2 divulgadas públicamente), dichas vulnerabilidades de zero-day son las siguientes:

- **Vulnerabilidad zero-day explotada activamente:**

CVE-2025-62221: Es una vulnerabilidad importante de elevación de privilegios que afecta al controlador de minifiltro de Windows Cloud Files y tiene una puntuación CVSS de 7.8 . Esta vulnerabilidad permite a atacantes locales autenticados con privilegios bajos elevar sus privilegios al nivel de SISTEMA explotando una vulnerabilidad de uso después de la liberación en el controlador de minifiltro de Windows Cloud Files mediante acceso local al sistema.

Existe evidencia de explotación activa. Microsoft ha confirmado la detección de la explotación, aunque la vulnerabilidad no se ha divulgado públicamente ni se han compartido detalles específicos sobre los métodos de explotación.

La vulnerabilidad afecta a sistemas Windows que ejecutan el controlador de minifiltro de Cloud Files y requiere acceso local, privilegios bajos y ninguna interacción del usuario para explotarla, con una complejidad de ataque baja. Si se explota con éxito, permite a los atacantes obtener privilegios de sistema, lo que podría comprometer por completo los sistemas Windows afectados. Microsoft ha publicado una solución oficial para abordar esta vulnerabilidad. Las organizaciones deben priorizar la aplicación de la actualización de seguridad disponible para protegerse contra la explotación.

La agencia CISA ha ordenado a las agencias federales de EE.UU. parchar esto antes del 30 de diciembre.

Vulnerabilidades zero-day de divulgación publica:

CVE-2025-64671: Es una vulnerabilidad importante de ejecución remota de código que afecta a GitHub Copilot para JetBrains y tiene una puntuación CVSS de 8,4 . Esta

vulnerabilidad permite a atacantes locales no autenticados ejecutar código arbitrario aprovechando una vulnerabilidad de inyección de comandos en Copilot mediante acceso local al sistema.

Si bien la vulnerabilidad se ha divulgado públicamente, no hay evidencia de explotación activa. Microsoft ha evaluado la explotación como "Menos probable" con una calificación de madurez del código de explotación no probada. La vulnerabilidad afecta a GitHub Copilot para JetBrains y no requiere privilegios ni interacción del usuario para su explotación, con una complejidad de ataque baja. Un atacante podría explotar esta vulnerabilidad mediante una inyección maliciosa de mensajes cruzados en archivos no confiables o servidores MCP, lo que le permitiría ejecutar comandos adicionales añadiéndolos a los comandos permitidos en la configuración de aprobación automática del terminal del usuario.

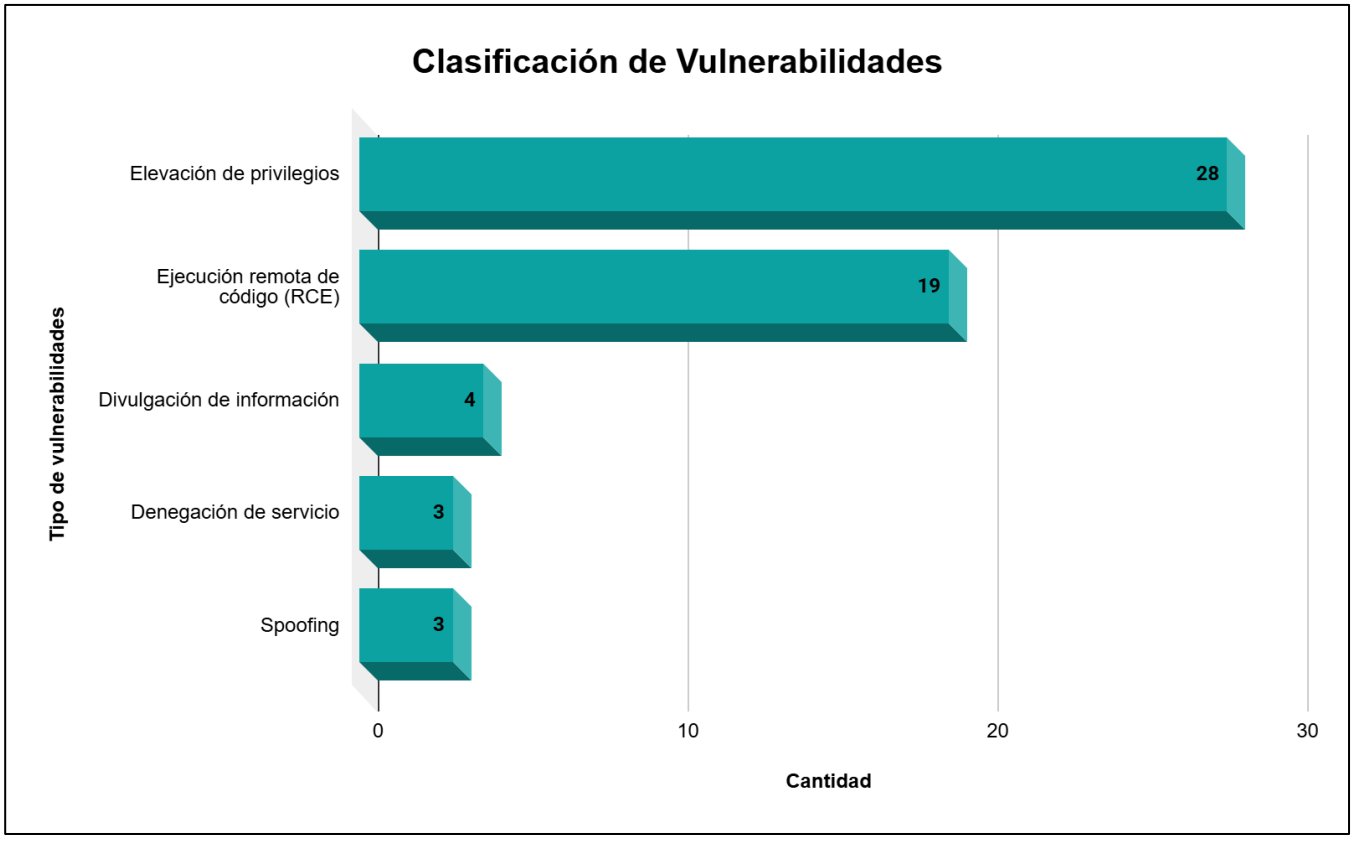
CVE-2025-54100: Es una vulnerabilidad importante de ejecución remota de código que afecta a Windows PowerShell y tiene una puntuación CVSS de 7,8 . Esta vulnerabilidad permite a atacantes locales no autenticados ejecutar código arbitrario aprovechando una vulnerabilidad de inyección de comandos en PowerShell mediante acceso local al sistema.

Si bien la vulnerabilidad se ha divulgado públicamente, no hay evidencia de explotación activa. Microsoft ha evaluado la explotación como "Menos probable" con una calificación de madurez del código de explotación no probada. La vulnerabilidad afecta a Windows PowerShell y no requiere privilegios, pero sí la interacción del usuario para explotarla, con una complejidad de ataque baja. Un atacante podría explotar esta vulnerabilidad mediante tácticas de ingeniería social, como convencer a la víctima para que descargue y ejecute un archivo malicioso o ejecute un comando de PowerShell especialmente diseñado, lo que provoca la ejecución de código en su sistema local.

- Distribución de Vulnerabilidades

Con respecto al total de las vulnerabilidades reportadas por Microsoft se encuentran categorizadas de la siguiente manera según el tipo:

- Elevación de privilegios: 28.
- Ejecución remota de código (RCE): 19.
- Divulgación de información: 4.
- Denegación de servicio: 3.
- Spoofing: 3



Principales vulnerabilidades críticas:

De acuerdo con él score o puntación de las vulnerabilidades y su probabilidad de explotación se tiene las siguientes vulnerabilidades críticas sobre las cuales se tiene que actuar inmediatamente en caso de presentar el componente afectado.

- CVE-2025-62562
- CVE-2025-62554
- CVE-2025-62557

- CVE-2025-62554 y CVE-2025-62557: son vulnerabilidades críticas de ejecución remota de código en Microsoft Office, ambas con puntuaciones CVSS de 8,4 . Estas vulnerabilidades permiten a atacantes no autenticados ejecutar código arbitrario explotando una debilidad de confusión de tipos (CVE-2025-62554) y una condición de uso tras liberación (CVE-2025-62557) en los componentes de Microsoft Office. La explotación no requiere la interacción del usuario en el peor de los casos y puede activarse enviando correos electrónicos o enlaces maliciosos especialmente diseñados al usuario objetivo.

A pesar de estar marcada como "Menos probable" de ser explotada, Microsoft señala que el panel de vista previa es un vector de ataque para ambas vulnerabilidades, lo que significa que la explotación no requiere que el usuario abra el archivo. Según los avisos de Microsoft, las actualizaciones de seguridad para Microsoft Office LTSC para Mac aún no están disponibles y se publicarán en cuanto estén listas.

- CVE-2025-62562: es una vulnerabilidad de tipo Use-After-Free (Uso de memoria después de liberarse). Este tipo de error ocurre cuando el programa (Outlook) intenta acceder a una sección de la memoria del sistema que ya ha sido liberada o borrada, lo que genera un comportamiento inestable que los atacantes pueden manipular.

Un atacante envía un correo electrónico malicioso que contiene archivos adjuntos o elementos manipulados específicamente para explotar este fallo de memoria

La vulnerabilidad puede activarse cuando el usuario abre el correo o, en algunos escenarios, simplemente cuando el correo se procesa en el Panel de Vista Previa de Outlook, sin necesidad de abrirlo completamente.

Si la explotación tiene éxito, el atacante puede ejecutar código arbitrario con los mismos permisos que el usuario local. Si el usuario tiene permisos de administrador, el atacante podría tomar control total del sistema (instalar programas, ver/borrar datos, crear nuevas cuentas).

Recursos y versiones afectadas:

Las vulnerabilidades abordadas en el Patch Tuesday de diciembre de 2025 impactan un amplio conjunto de productos y versiones de Microsoft, incluyendo tanto sistemas operativos cliente como servidor, así como diversas aplicaciones y componentes de la suite Microsoft Office. Entre los recursos afectados se encuentran:

- Windows 10 / 11 y Windows Server (2008 en adelante).
- Microsoft Office (Word, Excel, Outlook).
- Microsoft Exchange Server.
- Azure Monitor y componentes de Azure.
- PowerShell 5.1.

En la mayoría de los casos, Microsoft ha publicado actualizaciones de seguridad acumulativas que corrigen las vulnerabilidades en todas las ramas con soporte activo. Se recomienda a las entidades verificar el inventario de sus activos para identificar los sistemas y versiones que utilicen estos componentes y proceder con la instalación de las actualizaciones correspondientes.

Vector de impacto:

- Elevación de Privilegios (EoP)

Este fue el vector de impacto más predominante, con alrededor de 28 vulnerabilidades. Una vulnerabilidad de elevación de privilegios permite a un atacante con acceso limitado a un sistema obtener mayores privilegios, como los de un administrador. Esto a menudo se utiliza como un segundo paso después de haber obtenido un acceso inicial, para así tomar control total del sistema afectado.

- Ejecución Remota de Código (RCE)

Se corrigieron aproximadamente 19 vulnerabilidades de este tipo. Las vulnerabilidades de RCE son particularmente críticas porque permiten a un atacante ejecutar código malicioso en un sistema vulnerable a través de una red, sin necesidad de acceso físico. Esto puede llevar al compromiso total del sistema.

- Divulgación de información

Se abordaron cerca de 04 vulnerabilidades de este tipo. Estas fallas de seguridad podrían permitir a un atacante acceder a información sensible que normalmente estaría protegida en un sistema.

- Denegación de Servicio (DoS)

También se solucionaron alrededor de 3 vulnerabilidades de DoS. Un ataque de denegación de servicio tiene como objetivo hacer que un sistema o servicio no esté disponible para sus usuarios legítimos, interrumpiendo su funcionamiento.

- Suplantación de Identidad (Spoofing)

Finalmente, se corrigieron unas 3 vulnerabilidades de este tipo, las cuales podrían permitir a un atacante hacerse pasar por otra persona o sistema para ganar la confianza de un usuario y robar información o realizar otras acciones maliciosas.

Recomendaciones de mitigación:

- Aplicar de inmediato las actualizaciones de seguridad de diciembre de 2025 publicadas por Microsoft.
- Priorizar la aplicación de parches, debido a la existencia de vulnerabilidades activamente explotadas, es crucial aplicar estas actualizaciones lo antes posible, especialmente en sistemas críticos.
- Desplegar parches para el Zero-Day CVE-2025-62221 en todas las estaciones de trabajo y servidores Windows.
- Actualizar Microsoft Office en todos los endpoints de usuario final para mitigar el riesgo del "Panel de Vista Previa" (CVE-2025-62554).
- Recordar a los usuarios la importancia de no abrir archivos adjuntos ni hacer clic en enlaces sospechosos, especialmente teniendo en cuenta las vulnerabilidades que se explotan a través del panel de vista previa.
- si no se puede parchear se recomienda deshabilitar el Panel de Vista Previa en Outlook como medida de defensa en profundidad contra vulnerabilidades como la de Office.
- Instalar urgentemente KB5072033 vía Windows Update o Catálogo de Microsoft.

Los parches están disponibles a través de los canales habituales: Windows Update, Windows Server Update Services (WSUS) e Microsoft Endpoint Configuration Manager (MECM/Intune).

En cuanto a las actualizaciones suministradas para Windows 10 se debe recordar que no está disponibles para el público en general, sino que se pueden obtener si se tiene el servicio de

Windows 10 Enterprise LTSC o Programa ESU (Extended Security Updates), de no tener estos servicios se recomienda migrar los equipos a Windows 11.

Fuentes:

- https://thehackernews.com/2025/12/microsoft-issues-security-fixes-for-56.html
- https://www.redeszone.net/noticias/seguridad/actualizacion-microsoft-corrige-vulnerabilidades-criticas/
- https://cybersecuritynews.com/windows-powershell-0-day-vulnerability/
- https://threatprotect.qualys.com/2025/12/09/microsoft-patch-tuesday-december-2025-security-update-review/
- https://www.tenable.com/blog/microsofts-december-2025-patch-tuesday-addresses-56-cves-cve-2025-62221
- https://blog.tecnetone.com/martes-de-parches-de-microsoft-diciembre-2025
- https://msrc.microsoft.com/update-guide/releaseNote/2025-Dec.

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 893 1490 - 318 155 3570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.