Alerta ID:	0062
Fecha del reporte:	12-11-2025
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades en Patch Tuesday de Microsoft – noviembre 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 noviembre 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 11 de noviembre de 2025, Microsoft publicó su paquete mensual de actualizaciones de seguridad, abordando 63 vulnerabilidades incluyendo Windows, Office, Azure, SQL Server, Hyper-V, Visual Studio y más.

De las 63 vulnerabilidades reportadas por Microsoft se catalogaron 5 de nivel “criticas” y 58 importantes.

Adicionalmente se incluye una vulnerabilidad tipo zero-day que al día de hoy se encuentra activamente explotada, la cual es la siguiente:

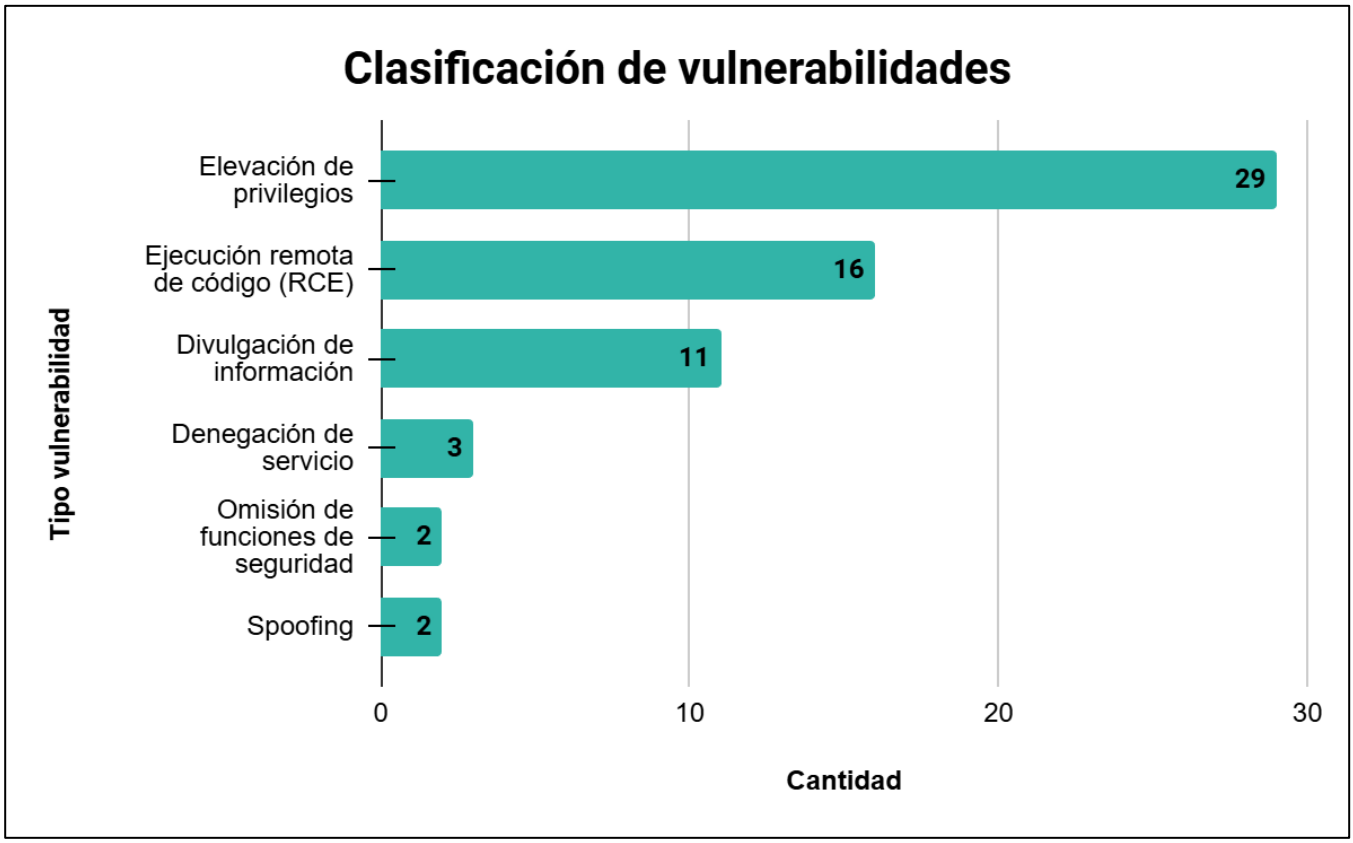
- CVE-2025-62215: Es una vulnerabilidad de fin de protección (EoP) en el kernel de Windows. Se le asignó una puntuación CVSSv3 de 7.0 y se clasificó como importante. Un atacante local autenticado podría explotar esta vulnerabilidad aprovechando una condición de carrera para obtener privilegios de SYSTEM. Según Microsoft, esta vulnerabilidad fue explotada en la práctica como una vulnerabilidad de día cero.

  Microsoft ha atribuido la vulnerabilidad al Centro de Inteligencia de Amenazas de Microsoft (MSTIC) y al Centro de Respuesta de Seguridad de Microsoft (MSRC), pero no ha compartido cómo se explotó la vulnerabilidad.

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: 29.
- Ejecución remota de código (RCE): 16.
- Divulgación de información: 11.
- Denegación de servicio: 3.
- Omisión de funciones de seguridad: 2.
- Spoofing: 2



Principales vulnerabilidades críticas:

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

MICROSOFT TAG	CVE	CVSS	Tipo
Componente gráfico de Microsoft	CVE-2025-60724	9.8	Elevación de privilegios en el kernel de gráficos DirectX
Nuance PowerScribe	CVE-2025-30398	8.1	Divulgación de información de Nuance PowerScribe 360
Microsoft Office	CVE-2025-62199	7.8	Ejecución remota de código en Microsoft Office
Windows DirectX	CVE-2025-60716	7.0	elevación de privilegios en el kernel de gráficos DirectX
Visual Studio	CVE-2025-62214	6.7	Vulnerabilidad de ejecución remota de código en Visual Studio

- CVE-2025-60724 es una vulnerabilidad de ejecución remota de código (RCE) en GDI+, con una puntuación CVSS 3.1 de 9.8. Esta vulnerabilidad se caracteriza por un desbordamiento de búfer basado en montón en el componente gráfico de Microsoft, lo que permite a un atacante no autorizado ejecutar código a través de la red. La vulnerabilidad puede explotarse engañando a la víctima para que descargue y abra un documento que contiene un metarchivo especialmente diseñado. En el peor de los casos, un atacante podría explotar esta vulnerabilidad en servicios web cargando documentos que contengan dicho metarchivo sin interacción del usuario. El atacante no requiere privilegios en los sistemas que alojan los servicios web. La explotación exitosa de esta vulnerabilidad podría provocar la ejecución remota de código o la divulgación de información en servicios web que analizan documentos que contienen el metarchivo, sin la participación del usuario. Microsoft ha evaluado la complejidad del ataque como "baja" y la probabilidad de explotación como "poco probable".

- CVE-2025-30398 es una vulnerabilidad de divulgación de información en Nuance PowerScribe 360, con una puntuación CVSS 3.1 de 8.1. La falta de autorización en Nuance PowerScribe permite que un atacante no autorizado divulgue información a través de la red. Un atacante no autenticado podría aprovechar esta vulnerabilidad realizando una llamada a la API de un punto de conexión específico. Posteriormente, el atacante podría usar los datos para acceder a información confidencial (incluidos datos personales) en el servidor. Microsoft evaluó que la complejidad del ataque es baja y que la explotación es poco probable.

- CVE-2025-62199 es una vulnerabilidad de ejecución remota de código (RCE) en aplicaciones de Microsoft Office, con una puntuación CVSS 3.1 de 7.8. Esta vulnerabilidad de uso después de liberación (use-after-free) en Microsoft Office permite que un atacante no autenticado ejecute código localmente en una estación de trabajo vulnerable. Para explotar esta vulnerabilidad, el atacante debe enviar al usuario un archivo malicioso y convencerlo de que lo abra. Microsoft ha evaluado que la complejidad del ataque es baja y que la explotación es poco probable.

- CVE-2025-60716 es una vulnerabilidad de elevación de privilegios en el kernel de DirectX Graphics, con una puntuación CVSS 3.1 de 7. Esta vulnerabilidad, caracterizada por un fallo de uso después de liberación en Windows DirectX, permite a un atacante autorizado elevar privilegios localmente. Para explotarla con éxito, el atacante debe superar una condición de carrera. Microsoft ha evaluado que la complejidad del ataque es «alta» y que la explotación es «poco probable».

- CVE-2025-62214 es una vulnerabilidad de ejecución remota de código (RCE) en Visual Studio, con una puntuación CVSS 3.1 de 6.7. Esta vulnerabilidad permite la inyección de comandos mediante IA en Visual Studio, lo que posibilita que un atacante autorizado ejecute código localmente. Su explotación no es trivial, ya que requiere varios pasos: inyección de prompts, interacción con el agente Copilot y la activación de una compilación. Microsoft ha evaluado la complejidad del ataque como «alta» y la probabilidad de explotación como «baja».

Recursos y versiones afectadas:

Las vulnerabilidades abordadas en el Patch Tuesday de noviembre 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:

- Sistemas Operativos Windows (10, 11, y versiones de Server 2016-2025)
- Microsoft Office
- Kernel de Windows
- Componente Gráfico de Windows (GDI+)
- Windows Subsystem for Linux (WSL)
- Visual Studio
- .NET

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 29 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.

Un ejemplo destacado de este mes es CVE-2025-62215, esta vulnerabilidad es la que fue catalogada como vulnerabilidad de zero-day que afecta el kernel de windows, en la cual un atacante te envía un correo de phishing con un archivo adjunto (como un PDF o un script) el cual al ser abierto el malware se instala, pero solo tiene los permisos limitados de la cuenta de usuario. En este punto, el atacante explota la CVE-2025-62215. La cual permite en el Kernel

(el núcleo del sistema) le permite "elevar" los permisos de "Usuario" a "SISTEMA" (el nivel más alto). Ahora, el atacante tiene control sobre la máquina en donde puede desactivar antivirus, robar las contraseñas de todos los usuarios e instalar un ransomware.

- Ejecución Remota de Código (RCE)

Se corrigieron aproximadamente 16 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.

Una vulnerabilidad crítica de este tipo es CVE-2025-62199 en Microsoft Office en donde un atacante envía un correo electrónico con un archivo de Office (Word, Excel) malicioso en donde ni siquiera se requiere abrir el archivo, solamente si el Outlook tiene el "Panel de Vista Previa" activado, en el momento en que se da clic en el correo para leerlo, el panel intenta generar una vista previa del archivo. Al hacerlo se puede ejecutar un código malicioso en la maquina en segundo plano. Esto podría instalar un troyano para robar datos sin consentimiento del propietario del equipo.

- Divulgación de información

Se abordaron cerca de 11 vulnerabilidades de este tipo. Estas fallas de seguridad podrían permitir a un atacante acceder a información sensible que normalmente estaría protegida en un sistema.

- Omisión de Funciones de Seguridad

Con aproximadamente 2 vulnerabilidades, este vector de impacto se refiere a fallos que permiten a un atacante eludir las medidas de seguridad existentes en un sistema, como el cifrado o las políticas de acceso.

- 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 2 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 noviembre 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.
- Atención especial en la vulnerabilidad CVE-2025-62215 Aplique la actualización en todos los sistemas Windows (estaciones de trabajo y servidores) de forma inmediata.
- Despliegue los parches para CVE-2025-60724 (GDI+) y CVE-2025-62199 (Office) con la misma urgencia, especialmente en estaciones de trabajo de usuarios que manejan correo electrónico y documentos.
- 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 (CVE-2025-62199).

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

Fuentes:

- https://winbuzzer.com/2025/11/12/microsoft-november-2025-patch-tuesday-fixes-actively-exploited-zero-day-63-vulnerabilities-xcxwbn/
- https://threatprotect.qualys.com/2025/11/11/microsoft-patch-tuesday-november-2025-security-update-review/
- https://www.softzone.es/noticias/windows/parches-seguridad-noviembre-2025/
- https://blog.talosintelligence.com/microsoft-patch-tuesday-november-2025/
- https://cybersecuritynews.com/microsoft-november-2025-patch-tuesday/
- https://www.tenable.com/blog/microsofts-november-2025-patch-tuesday-addresses-63-cves-cve-2025-62215
- https://www.crowdstrike.com/en-us/blog/patch-tuesday-analysis-november-2025/

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.