Alerta ID:	0044
Fecha del reporte:	15-10-2025
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades en Patch Tuesday de Microsoft – octubre 2025
Herramienta de detección	Análisis de fuentes oficiales (Microsoft, BleepingComputer, etc)
Activo involucrado:	Sistemas operativos Microsoft Windows y componentes asociados (Windows Server, Exchange Server, WSUS, BitLocker, Windows NTFS, Windows NTLM, Microsoft Office, entre otros), plataformas en la nube y servicios de azure, 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 octubre 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 14 de octubre de 2025, Microsoft publicó su paquete mensual de actualizaciones de seguridad, abordando 175 vulnerabilidades, de las cuales 5 son críticas y 121 importantes.

Se identificaron 6 vulnerabilidades de “día cero”, de las cuales 2 ya estaban siendo explotadas activamente, las cuales son:

- **CVE-2025-24990:** Afecta al controlador de módem Agere ltmdm64.sys heredado, eliminado por Microsoft. Permite a atacantes locales obtener privilegios administrativos mediante una desreferencia de puntero no confiable.

- **CVE-2025-59230**: Afecta al Administrador de Conexión de Acceso Remoto por control de acceso inadecuado, permitiendo escalada de privilegios locales al nivel del SISTEMA.

Las otras vulnerabilidades de “día cero” reportadas son las siguientes:

- **CVE-2025-47827 – Bypass de Secure Boot en IGEL OS**

Permite montar sistemas de archivos no verificados, comprometiendo el arranque seguro.

Afecta IGEL OS antes de la versión 11.

- **CVE-2025-0033 – Corrupción de memoria en AMD SEV-SNP**

Vulnerabilidad en procesadores AMD EPYC con virtualización segura.

Permite manipulación de memoria protegida en entornos Azure Confidential Computing.

El parche aún está en despliegue para clusters Azure. [bleepingcomputer.com]

- **CVE-2025-24052 – Elevación de privilegios en Agere Modem Driver**

Similar a CVE-2025-24990, pero no explotada activamente al momento del parche. [petri.com]

- **CVE-2025-2884 – Lectura fuera de límites en TCG TPM2.0**

Permite divulgación de información o denegación de servicio en módulos TPM

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:** 84.
- **Ejecución remota de código (RCE):** 31.
- **Divulgación de información:** 28.
- **Bypass de funciones de seguridad:** 11.
- **Denegación de servicio:** 11.
- **Suplantación (Spoofing):** 10.

Se anexa archivo en formato en Excel en donde se encuentran todas las vulnerabilidades presentadas por Microsoft en "Patch Tuesday"

Principales vulnerabilidades críticas:

De acuerdo a él score o puntación de las vulnerabilidades se tiene las siguientes vulnerabilidades críticas con un CVSS superior a 9 y sobre las cuales se tiene que actuar inmediatamente en caso de presentar el componente afectado son las siguientes.

MICROSOFT TAG	CVE	CVSS	Tipo
Microsoft Graphics Component	CVE-2025-49708	9.9	Elevación de privilegios (componente gráfico de Microsoft)
ASP.NET Core	CVE-2025-55315	9.9	omisión de funciones de seguridad (ASP.NET)
Azure Entra ID	CVE-2025-59218	9.6	elevación de privilegios (ID de Azure Entra)
Azure Entra ID	CVE-2025-59246	9.8	elevación de privilegios (ID de Azure Entra)
Windows Server Update Service	CVE-2025-59287	9.8	ejecución remota de código (WSUS)

Recursos y versiones afectadas:

Las vulnerabilidades abordadas en el Patch Tuesday de octubre 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:

Las actualizaciones de este mes cubren una amplia gama de productos de Microsoft:

- **Sistemas Operativos Windows:** Se han lanzado actualizaciones para todas las versiones soportadas de Windows. Este mes marca la **última actualización de seguridad para Windows 10**, que llega a su fin de soporte. A partir de ahora, los usuarios que no migren a Windows 11 deberán acogerse al programa de Actualizaciones de Seguridad Extendidas (ESU) para seguir recibiendo parches, también se hay afectación en componentes de Windows Server a nivel de Kernel, NTFS, NTLM, Remote Desktop, BitLocker, Hyper-V, SMB, TCP/IP, LSASS, DWM, Win32k, Firewall, Connected Devices Platform Service.
- **Microsoft Office:** Se han solucionado varias vulnerabilidades, incluyendo las mencionadas de ejecución remota de código. También es importante destacar que **Office 2016 y Office 2019 llegan al final de su ciclo de vida** este mes.
- **Microsoft Exchange Server:** Se han publicado actualizaciones de seguridad que abordan vulnerabilidades de elevación de privilegios y suplantación de identidad (CVE-2025-59249, CVE-2025-53782, CVE-2025-59248). Aunque no se tiene constancia de su explotación activa, se recomienda su instalación inmediata. Al igual que Office, **Exchange Server 2016 y 2019 también han llegado al fin de su soporte**.
- **Componentes del Kernel de Windows:** Se ha corregido una gran cantidad de vulnerabilidades de elevación de privilegios, incluyendo **CVE-2025-59194** en el propio Kernel de Windows.
- **Azure:** Se han solucionado múltiples vulnerabilidades en servicios como Azure Entra ID, Azure Monitor Agent, Azure Arc y Azure Compute Gallery.

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.

También se debe tener en consideración que dentro de la alertar reportadas por Microsoft se encuentra la de finalización de soporte de las siguientes plataformas y aplicaciones.

- **Windows 10:** Última actualización gratuita (KB5066791). Solo recibirá parches críticos mediante ESU.
- **Office 2016/2019, Exchange Server 2016/2019:** Fin de soporte oficial.

Vector de impacto:

- Elevación de Privilegios (EoP)

Este fue el vector de impacto más predominante, con alrededor de **84 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-2025-59230, una vulnerabilidad en el Administrador de Conexiones de Acceso Remoto de Windows que ya está siendo explotada activamente.

- Ejecución Remota de Código (RCE)

Se corrigieron aproximadamente **31 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-2025-59287** en Windows Server Update Service (WSUS), la cual podría permitir a un atacante tomar control del servidor de actualizaciones.

- Revelación de Información

Se abordaron cerca de **28 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 **11 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 **11 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 **10 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 octubre 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 a WSUS y servidores Exchange, la vulnerabilidad en WSUS (CVE-2025-59287) es de máxima prioridad. Los administradores de Exchange deben aplicar las actualizaciones correspondientes sin demora.

- Planificar la migración de productos sin soporte: Con el fin de vida de Windows 10, Office 2016/2019 y Exchange 2016/2019, las entidades deben tener un plan claro para migrar a versiones más nuevas y soportadas o contratar el programa ESU para Windows 10 si es necesario.
- 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.
- Desplegar de manera urgente y prioritaria las actualizaciones que corrigen CVE-2025-59230 (RasMan) y CVE-2025-24990 (Controlador Agere) en todos los equipos de usuario (endpoints) y servidores Windows.
- Consideración Específica (CVE-2025-24990): El parche elimina el controlador ltmdm64.sys. Identifica si en tu organización existen sistemas de hardware legados (como módems de fax analógicos) que dependan de este controlador para evaluar el impacto funcional, aunque la seguridad debe prevalecer.

- Desplegar las actualizaciones para Office que corrigen CVE-2025-59227 y CVE-2025-59234.
- Aplica de inmediato las actualizaciones de seguridad para Exchange (CVE-2025-59249, etc.). No esperes al ciclo de parcheo regular. Estos servidores son un objetivo de alto valor para los atacantes.
- Dado que se está explotando una vulnerabilidad en el servicio RasMan (Remote Access), presta especial atención a los servidores que gestionan conexiones remotas (VPN, DirectAccess), ya que son un perímetro de entrada.

Fuentes:

- https://www.tenable.com/blog/microsofts-october-2025-patch-tuesday-addresses-167-cves-cve-2025-24990-cve-2025-59230
- https://blog.segu-info.com.ar/2025/10/actualizaciones-de-seguridad-de-octubre.html
- https://orain.eus/es/ikusmiran/tecnologia/2025/10/13/guia-salvar-tu-windows-10/
- https://www.bleepingcomputer.com/news/microsoft/microsoft-october-2025-patch-tuesday-fixes-6-zero-days-172-flaws/
- https://msrc.microsoft.com/update-guide/vulnerability

- https://csirt.telconet.net/comunicacion/noticias-seguridad/actualizacion-de-patch-tuesday-de-microsoft-octubre-2025/
- https://www.splashtop.com/es/blog/patch-tuesday-october-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.