CSIRT Salud

Boletín informativo

CSIRTSALUD-AL-20250911-28

TLP: CLEAR

Alerta ID:	0028
Fecha del reporte:	11-09-2025
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades en Patch Tuesday de Microsoft – Septiembre 2025
Herramienta de detección	Análisis de fuentes oficiales (Microsoft, BleepingComputer, etc)
Activo involucrado:	Sistemas operativos Microsoft Windows y componentes asociados (Windows Server, Windows Hyper-V, Windows SMB, Windows NTFS, Windows NTLM, Microsoft Office, Microsoft SharePoint, Microsoft High Performance Compute Pack, entre otros).
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 septiembre de 2025, con el fin de concientizar sobre los riesgos de explotación, facilitar la identificación de activos y versiones afectados, promover la aplicación oportuna de parches y medidas de mitigación, y fortalecer la capacidad de respuesta ante incidentes de seguridad que puedan comprometer la confidencialidad, integridad y disponibilidad de los sistemas institucionales.

Descripción:

El 09 de septiembre de 2025, Microsoft publicó su paquete mensual de actualizaciones de seguridad (Patch Tuesday), abordando **81 vulnerabilidades**, de las cuales **8 son críticas y 72 importantes**.

Aunque no se han reportado vulnerabilidades explotadas activamente hasta el momento, varias fueron catalogadas como **"más probables de ser explotadas"**, incluyendo vulnerabilidades de **elevación de privilegios (EoP)**, **ejecución remota de código (RCE)** y **divulgación de información** en múltiples componentes de Windows y Microsoft Office.

Destaca especialmente la vulnerabilidad **CVE-2025-55234 (Windows SMB)**, que fue **divulgada públicamente antes del parche** y podría permitir **ataques de relay y escalamiento de privilegios** si no se aplican las configuraciones de endurecimiento recomendadas. También resalta **CVE-2025-54918 (Windows NTLM)**, clasificada como crítica y **más probable de ser explotada**, la cual permite elevar privilegios a SYSTEM en sistemas vulnerables.

La explotación de estas fallas podría permitir a un atacante moverse lateralmente, desplegar ransomware, robar información o comprometer de forma persistente los sistemas afectados.

Principales vulnerabilidades críticas:

CVE	CVSS	Tipo
CVE-2025-54918	8.8	Elevación de privilegios (Windows NTLM) (Tenable®)
CVE-2025-54910	8.4	Ejecución remota de código (Microsoft Office) (Tenable®)

CVE	CVSS	Tipo
CVE-2025-55224	7.8	Ejecución remota de código (Windows Hyper-V) (Tenable®)
CVE-2025-55232	9.8	Ejecución remota de código (High Performance Compute Pack) (Tenable®)
CVE-2025-55226	7.8	Ejecución remota de código (Graphics Kernel) (Lansweeper)
CVE-2025-53800	7.8	Elevación de privilegios (Windows Graphics Component) (Petri IT Knowledgebase)
CVE-2025-55236	*	Remote Code Execution (Graphics Kernel) — severidad crítica según informe de productos afectados (Lansweeper)
CVE-2025-55241	*	Elevación de privilegios (Azure Entra) — listado entre los críticos (Redmondmag)

Recursos y versiones afectadas:

Las vulnerabilidades abordadas en el Patch Tuesday de septiembre 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 cliente y servidor, incluyendo Windows 10 (múltiples ediciones), Windows 11 (22H2, 23H2 y 24H2), Windows Server 2012, 2016, 2019, 2022 y 2025.

- Servicios y componentes del sistema operativo, como SMB, NTLM, NTFS, Hyper-V, Kernel, TCP/IP, LSASS, RRAS, DWM, BitLocker, Win32k, Defender Firewall y Connected Devices Platform Service, entre otros.

- Aplicaciones de productividad y colaboración, como Microsoft Office (Word, Excel, PowerPoint, Visio, SharePoint), Microsoft SQL Server y el agente de máquinas virtuales de Azure (Azure Windows Virtual Machine Agent).

- Plataformas de virtualización y nube, como Windows Hyper-V y Azure Arc.

- Componentes gráficos y de interfaz de usuario, incluidos Microsoft Graphics Component, Windows UI XAML y Graphics Kernel.

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:

- Compromiso de la confidencialidad, integridad y disponibilidad de los sistemas.

- Escalada de privilegios desde cuentas estándar hasta privilegios de SYSTEM.

- Ejecución remota de código no autorizado.

- Posible movimiento lateral y despliegue de ransomware en redes corporativas.

- Interrupción de servicios críticos de negocio.

Recomendaciones de mitigación:

- Aplicar de inmediato las actualizaciones de seguridad de septiembre de 2025 publicadas por Microsoft.
- Priorizar el parcheo de vulnerabilidades críticas y con mayor probabilidad de explotación (CVE-2025-55234, CVE-2025-54918, CVE-2025-54916, entre otras).
- Habilitar medidas de endurecimiento en SMB: habilitar SMB signing y Extended Protection for Authentication (EPA).
- Implementar segmentación de red y listas de control de acceso para restringir el alcance de ataques internos.
- Mantener respaldos actualizados y probar regularmente los planes de recuperación ante desastres.
- Realizar escaneos de vulnerabilidades frecuentes para identificar y corregir sistemas sin parchear.

Fuentes:

- https://cyberscoop.com/microsoft-patch-tuesday-september-2025/?utm_source=chatgpt.com
- https://csirt.telconet.net/comunicacion/noticias-seguridad/actualizacion-de-patch-tuesday-de-microsoft-septiembre-2025/
- https://thehackernews.com/2024/09/microsoft-issues-patches-for-79-flaws.html
- https://jp.tenable.com/blog/microsofts-september-2025-patch-tuesday-addresses-80-cves-cve-2025-55234?utm_source=chatgpt.com
- https://www.bleepingcomputer.com/news/microsoft/microsoft-september-2024-patch-tuesday-fixes-4-zero-days-79-flaws/

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.