Alerta ID:	0014
Fecha del reporte:	14-08-2025
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades críticas y Zero-Day en Patch Tuesday de Microsoft – Agosto 2025
Herramienta de detección	Análisis de fuentes oficiales (Microsoft, CISA, BleepingComputer)
Activo involucrado:	Microsoft Windows, Office, SharePoint Server, Hyper-V, SQL Server, Azure Stack Hub, Azure Virtual Machines
Tipo de incidente:	*Vulnerabilidad crítica y Zero-Day*
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del ecosistema digital sobre las vulnerabilidades críticas y un zero-day abordados en las actualizaciones de seguridad de Microsoft correspondientes al Patch Tuesday de agosto 2025, con el fin de priorizar su mitigación para evitar explotación activa que pueda derivar en pérdida de información, ejecución remota de código o elevación de privilegios.

Descripción:

Microsoft ha publicado su actualización mensual de seguridad, corrigiendo un total de **107 vulnerabilidades**, de las cuales **13 han sido clasificadas como críticas**. Entre ellas se destaca una vulnerabilidad **Zero-Day (CVE-2025-53779)** en **Windows Kerberos**, que permite a un atacante autenticado escalar privilegios hasta administrador de dominio mediante un *path traversal*.

Clasificación de vulnerabilidades por tipo:

42 vulnerabilidades de elevación de privilegios.

35 vulnerabilidades de ejecución remota de código (RCE).

16 vulnerabilidades de divulgación de información.

4 vulnerabilidades de denegación de servicio (DoS).

8 vulnerabilidades de suplantación (Spoofing).

1 vulnerabilidad de Cross-Site Scripting.

1 vulnerabilidad de manipulación.

Principales vulnerabilidades críticas:

CVE	CVSS	Tipo
CVE-2025-53793	7.5	Divulgación de información en Azure Stack Hub
CVE-2025-49707	7.9	Spoofing en Azure Virtual Machines
CVE-2025-53781	7.7	Divulgación de información en Azure Virtual Machines
CVE-2025-50176	7.8	RCE en DirectX Graphics Kernel
CVE-2025-50165	9.8	RCE en Windows Graphics Component
CVE-2025-53740	8.4	RCE en Microsoft Office
CVE-2025-53731	8.4	RCE en Microsoft Office
CVE-2025-53784	8.4	RCE en Microsoft Word
CVE-2025-53733	8.4	RCE en Microsoft Word
CVE-2025-48807	7.5	RCE en Windows Hyper-V
CVE-2025-53766	9.8	RCE en Windows GDI+
CVE-2025-50177	8.1	RCE en Microsoft Message Queuing (MSMQ)
CVE-2025-53778	8.8	Elevación de privilegios en Windows NTLM

Listado completo de vulnerabilidades:

Tag	CVE ID	CVE Title	Severity
Azure File Sync	CVE-2025-53729	Microsoft Azure File Sync Elevation of Privilege Vulnerability	Important
Azure Stack	CVE-2025-53793	Azure Stack Hub Information Disclosure Vulnerability	Critical
Azure Stack	CVE-2025-53765	Azure Stack Hub Information Disclosure Vulnerability	Important

Tag	CVE ID	CVE Title	Severity
Azure Virtual Machines	CVE-2025-49707	Azure Virtual Machines Spoofing Vulnerability	Critical
Azure Virtual Machines	CVE-2025-53781	Azure Virtual Machines Information Disclosure Vulnerability	Critical
Desktop Windows Manager	CVE-2025-53152	Desktop Windows Manager Remote Code Execution Vulnerability	Important
Desktop Windows Manager	CVE-2025-50153	Desktop Windows Manager Elevation of Privilege Vulnerability	Important
GitHub Copilot and Visual Studio	CVE-2025-53773	GitHub Copilot and Visual Studio Remote Code Execution Vulnerability	Important
Graphics Kernel	CVE-2025-50176	DirectX Graphics Kernel Remote Code Execution Vulnerability	Critical
Kernel Streaming WOW Thunk Service Driver	CVE-2025-53149	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	Important
Kernel Transaction Manager	CVE-2025-53140	Windows Kernel Transaction Manager Elevation of Privilege Vulnerability	Important
Microsoft Brokering File System	CVE-2025-53142	Microsoft Brokering File System Elevation of Privilege Vulnerability	Important
Microsoft Dynamics 365 (on-premises)	CVE-2025-49745	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	Important

Tag	CVE ID	CVE Title	Severity
Microsoft Dynamics 365 (on-premises)	CVE-2025-53728	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability	Important
Microsoft Edge for Android	CVE-2025-49755	Microsoft Edge (Chromium-based) for Android Spoofing Vulnerability	Low
Microsoft Edge for Android	CVE-2025-49736	Microsoft Edge (Chromium-based) for Android Spoofing Vulnerability	Moderate
Microsoft Exchange Server	CVE-2025-25005	Microsoft Exchange Server Tampering Vulnerability	Important
Microsoft Exchange Server	CVE-2025-25006	Microsoft Exchange Server Spoofing Vulnerability	Important
Microsoft Exchange Server	CVE-2025-25007	Microsoft Exchange Server Spoofing Vulnerability	Important
Microsoft Exchange Server	CVE-2025-53786	Microsoft Exchange Server Hybrid Deployment Elevation of Privilege Vulnerability	Important
Microsoft Exchange Server	CVE-2025-33051	Microsoft Exchange Server Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2025-49743	Windows Graphics Component Elevation of Privilege Vulnerability	Important
Microsoft Graphics Component	CVE-2025-50165	Windows Graphics Component Remote Code Execution Vulnerability	Critical

Tag	CVE ID	CVE Title	Severity
Microsoft Office	CVE-2025-53732	Microsoft Office Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2025-53740	Microsoft Office Remote Code Execution Vulnerability	Critical
Microsoft Office	CVE-2025-53731	Microsoft Office Remote Code Execution Vulnerability	Critical
Microsoft Office Excel	CVE-2025-53759	Microsoft Excel Remote Code Execution Vulnerability	Important
Microsoft Office Excel	CVE-2025-53737	Microsoft Excel Remote Code Execution Vulnerability	Important
Microsoft Office Excel	CVE-2025-53739	Microsoft Excel Remote Code Execution Vulnerability	Important
Microsoft Office Excel	CVE-2025-53735	Microsoft Excel Remote Code Execution Vulnerability	Important
Microsoft Office Excel	CVE-2025-53741	Microsoft Excel Remote Code Execution Vulnerability	Important
Microsoft Office PowerPoint	CVE-2025-53761	Microsoft PowerPoint Remote Code Execution Vulnerability	Important
Microsoft Office SharePoint	CVE-2025-53760	Microsoft SharePoint Elevation of Privilege Vulnerability	Important
Microsoft Office SharePoint	CVE-2025-49712	Microsoft SharePoint Remote Code Execution Vulnerability	Important

Tag	CVE ID	CVE Title	Severity
Microsoft Office Visio	CVE-2025-53730	Microsoft Office Visio Remote Code Execution Vulnerability	Important
Microsoft Office Visio	CVE-2025-53734	Microsoft Office Visio Remote Code Execution Vulnerability	Important
Microsoft Office Word	CVE-2025-53738	Microsoft Word Remote Code Execution Vulnerability	Important
Microsoft Office Word	CVE-2025-53736	Microsoft Word Information Disclosure Vulnerability	Important
Microsoft Office Word	CVE-2025-53784	Microsoft Word Remote Code Execution Vulnerability	Critical
Microsoft Office Word	CVE-2025-53733	Microsoft Word Remote Code Execution Vulnerability	Critical
Microsoft Teams	CVE-2025-53783	Microsoft Teams Remote Code Execution Vulnerability	Important
Remote Access Point-to-Point Protocol (PPP) EAP-TLS	CVE-2025-50159	Remote Access Point-to-Point Protocol (PPP) EAP-TLS Elevation of Privilege Vulnerability	Important
Remote Desktop Server	CVE-2025-50171	Remote Desktop Spoofing Vulnerability	Important
Role: Windows Hyper-V	CVE-2025-50167	Windows Hyper-V Elevation of Privilege Vulnerability	Important

Tag	CVE ID	CVE Title	Severity
Role: Windows Hyper-V	CVE-2025-53155	Windows Hyper-V Elevation of Privilege Vulnerability	Important
Role: Windows Hyper-V	CVE-2025-49751	Windows Hyper-V Denial of Service Vulnerability	Important
Role: Windows Hyper-V	CVE-2025-53723	Windows Hyper-V Elevation of Privilege Vulnerability	Important
Role: Windows Hyper-V	CVE-2025-48807	Windows Hyper-V Remote Code Execution Vulnerability	Critical
SQL Server	CVE-2025-49758	Microsoft SQL Server Elevation of Privilege Vulnerability	Important
SQL Server	CVE-2025-24999	Microsoft SQL Server Elevation of Privilege Vulnerability	Important
SQL Server	CVE-2025-53727	Microsoft SQL Server Elevation of Privilege Vulnerability	Important
SQL Server	CVE-2025-49759	Microsoft SQL Server Elevation of Privilege Vulnerability	Important
SQL Server	CVE-2025-47954	Microsoft SQL Server Elevation of Privilege Vulnerability	Important
Storage Port Driver	CVE-2025-53156	Windows Storage Port Driver Information Disclosure Vulnerability	Important
Web Deploy	CVE-2025-53772	Web Deploy Remote Code Execution Vulnerability	Important

Tag	CVE ID	CVE Title	Severity
Windows Ancillary Function Driver for WinSock	CVE-2025-53718	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Important
Windows Ancillary Function Driver for WinSock	CVE-2025-53134	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Important
Windows Ancillary Function Driver for WinSock	CVE-2025-49762	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Important
Windows Ancillary Function Driver for WinSock	CVE-2025-53147	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Important
Windows Ancillary Function Driver for WinSock	CVE-2025-53154	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Important
Windows Ancillary Function Driver for WinSock	CVE-2025-53137	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Important
Windows Ancillary Function Driver for WinSock	CVE-2025-53141	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Important
Windows Cloud Files Mini Filter Driver	CVE-2025-50170	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Important

Tag	CVE ID	CVE Title	Severity
Windows Connected Devices Platform Service	CVE-2025-53721	Windows Connected Devices Platform Service Elevation of Privilege Vulnerability	Important
Windows DirectX	CVE-2025-53135	DirectX Graphics Kernel Elevation of Privilege Vulnerability	Important
Windows DirectX	CVE-2025-50172	DirectX Graphics Kernel Denial of Service Vulnerability	Important
Windows Distributed Transaction Coordinator	CVE-2025-50166	Windows Distributed Transaction Coordinator (MSDTC) Information Disclosure Vulnerability	Important
Windows File Explorer	CVE-2025-50154	Microsoft Windows File Explorer Spoofing Vulnerability	Important
Windows GDI+	CVE-2025-53766	GDI+ Remote Code Execution Vulnerability	Critical
Windows Installer	CVE-2025-50173	Windows Installer Elevation of Privilege Vulnerability	Important
Windows Kerberos	CVE-2025-53779	Windows Kerberos Elevation of Privilege Vulnerability	Moderate
Windows Kernel	CVE-2025-49761	Windows Kernel Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2025-53151	Windows Kernel Elevation of Privilege Vulnerability	Important

Tag	CVE ID	CVE Title	Severity
Windows Local Security Authority Subsystem Service (LSASS)	CVE-2025-53716	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability	Important
Windows Media	CVE-2025-53131	Windows Media Remote Code Execution Vulnerability	Important
Windows Message Queuing	CVE-2025-53145	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	Important
Windows Message Queuing	CVE-2025-53143	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	Important
Windows Message Queuing	CVE-2025-50177	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	Critical
Windows Message Queuing	CVE-2025-53144	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	Important
Windows NT OS Kernel	CVE-2025-53136	NT OS Kernel Information Disclosure Vulnerability	Important
Windows NTFS	CVE-2025-50158	Windows NTFS Information Disclosure Vulnerability	Important
Windows NTLM	CVE-2025-53778	Windows NTLM Elevation of Privilege Vulnerability	Critical
Windows PrintWorkflowUserSvc	CVE-2025-53133	Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability	Important

Tag	CVE ID	CVE Title	Severity
Windows Push Notifications	CVE-2025-53725	Windows Push Notifications Apps Elevation of Privilege Vulnerability	Important
Windows Push Notifications	CVE-2025-53724	Windows Push Notifications Apps Elevation of Privilege Vulnerability	Important
Windows Push Notifications	CVE-2025-50155	Windows Push Notifications Apps Elevation of Privilege Vulnerability	Important
Windows Push Notifications	CVE-2025-53726	Windows Push Notifications Apps Elevation of Privilege Vulnerability	Important
Windows Remote Desktop Services	CVE-2025-53722	Windows Remote Desktop Services Denial of Service Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2025-50157	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2025-53153	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2025-50163	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2025-50162	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Important

Tag	CVE ID	CVE Title	Severity
Windows Routing and Remote Access Service (RRAS)	CVE-2025-50164	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2025-53148	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2025-53138	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2025-50156	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2025-49757	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2025-53719	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2025-53720	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2025-50160	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Important

Tag	CVE ID	CVE Title	Severity
Windows Security App	CVE-2025-53769	Windows Security App Spoofing Vulnerability	Important
Windows SMB	CVE-2025-50169	Windows SMB Remote Code Execution Vulnerability	Important
Windows StateRepository API	CVE-2025-53789	Windows StateRepository API Server file Elevation of Privilege Vulnerability	Important
Windows Subsystem for Linux	CVE-2025-53788	Windows Subsystem for Linux (WSL2) Kernel Elevation of Privilege Vulnerability	Important
Windows Win32K - GRFX	CVE-2025-50161	Win32k Elevation of Privilege Vulnerability	Important
Windows Win32K - GRFX	CVE-2025-53132	Win32k Elevation of Privilege Vulnerability	Important
Windows Win32K - ICOMP	CVE-2025-50168	Win32k Elevation of Privilege Vulnerability	Important

Vector de impacto:

- Ejecución remota de código en sistemas Windows y aplicaciones Microsoft.
- Escalada de privilegios hasta administrador de dominio.
- Acceso no autorizado a información sensible.
- Compromiso de entornos virtualizados y servicios en la nube (Azure).

Recomendaciones de mitigación:

Pasos urgentes:

1. **Aplicar actualizaciones de seguridad** disponibles a través de:
    - *Windows Update*: Inicio → Configuración → Actualización de Windows → "Buscar actualizaciones".
    - *Catálogo de Microsoft Update*: https://www.catalog.update.microsoft.com
    - *Microsoft Security Update Guide*: https://msrc.microsoft.com/update-guide
2. **Priorizar la instalación de parches críticos**, especialmente para:
    - Windows Kerberos (CVE-2025-53779).
    - Windows GDI+ (CVE-2025-53766).
    - Windows Graphics Component (CVE-2025-50165).
3. **Actualizar componentes adicionales** como .NET Framework, Microsoft Office y SQL Server a las versiones más recientes.
4. **Reiniciar los sistemas** tras la aplicación de parches para completar la actualización.

Recomendaciones adicionales:

- Implementar un sistema de gestión de parches automatizado para garantizar cobertura completa.
- Monitorear los sistemas en busca de intentos de explotación.
- Mantener actualizados todos los controladores y dependencias críticas del sistema.

Fuentes:

- Microsoft Security Update Guide
- BleepingComputer – Microsoft August 2025 Patch Tuesday
- WindowsCentral – Novedades Patch Tuesday Agosto 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.