Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

PARCHE DE MICROSOFT DE AGOSTO DE 2025: CORRIGE VULNERABILIDAD DE DÍA CERO Y 108 FALLOS DE SEGURIDAD

12/ 08 / 2025

CONTENIDO

INTRODUCCIÓN

El Patch Tuesday de agosto de 2025 marca un evento crítico en el ciclo de mantenimiento de seguridad para organizaciones a nivel global. Microsoft ha publicado su boletín de seguridad mensual, el cual detalla una serie de actualizaciones y parches diseñados para abordar vulnerabilidades identificadas en sus productos y servicios.

PARCHE DE MICROSOFT DE AGOSTO DE 2025: CORRIGE VULNERABILIDAD DE DÍA CERO Y 108 FALLOS DE SEGURIDAD.

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_08_12_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	12/08/2025
Es día cero (0 day):	No

RESUMEN

Microsoft acaba de lanzar una serie de actualizaciones de seguridad que ayudaran a corregir 108 vulnerabilidades incluyendo una Zero-day.

De las 108 vulnerabilidades 13 son catalogadas como criticas:

- 9 permiten ejecución remota de código (RCE)
- 3 exponen información sensible
- 1 facilita la elevación de privilegios.

Clasificación de fallos

- Elevación de privilegios 43
- Ejecución de código remoto 35
- Divulgación de información 18
- Denegación de servicio 3
- Suplantación (Spoofing) 9

Zero-Day

La vulnerabilidad fue identificada como CVE-2025-53779 este afecta al componente Windows Kerberos y permite a un atacante autenticado alcanzar privilegios de administrador de dominio mediante una técnica de transversal de ruta relativa e la gestión de cuentas de servicio delegadas (dMSA).

Microsoft indica que el atacante necesita permisos sobre los atributos:

- msds-groupMSAMembership
- msds-ManagedAccountPrecededByLink

Aunque Microsoft considera que su explotación es menos probable, el impacto potencial control total del dominio lo vuelve muy grave.

Vulnerabilidades criticas

Según investigadores hay 4 vulnerabilidades que deberían de priorizar los equipos de TI las cuales son:

CVE-2025-53740 y CVE-2025-53731: Microsoft Office, es de tipo RCE y se explota vía Preview pane, da una vista previa del archivo en el explorador de correos, esto sin la necesidad de abrirlo por completo. Eso podría llegar a permitir ejecutar código automáticamente desde documentos maliciosos.

CVE-2025-50165: Componente gráfico de Windows, es de tipo RCE esta se activa al procesar una imagen JEPG malformada, sin privilegios ni interacción por parte del usuario, tiene un riesgo potencial de propagación de tipo gusano.

CVE-2025-53766: GDI+, es de tipo RCE por desbordamiento de búfer en memoria, es explotable con archivos gráficos maliciosos o documentos con metadatos, útil para los cibercriminales a la hora de buscar movimientos laterales o compromisos en cadena de suministro.

Etiqueta	CVE ID	Título	Criticidad
Azure Stack	CVE-2025-53793	Vulnerabilidad de divulgación de información de Azure Stack Hub	Crítico
Máquinas virtuales de Azure	CVE-2025-49707	Vulnerabilidad de suplantación de identidad de Azure Virtual Machines	Crítico
Máquinas virtuales de Azure	CVE-2025-53781	Vulnerabilidad de divulgación de información de Azure Virtual Machines	Crítico
Kernel de gráficos	CVE-2025-50176	Vulnerabilidad de ejecución remota de código del kernel de gráficos de DirectX	Crítico
Componente de gráficos de Microsoft	CVE-2025-50165	Vulnerabilidad de ejecución remota de código del componente de gráficos de Windows	Crítico
Microsoft Office	CVE-2025-53740	Vulnerabilidad de ejecución remota de código de Microsoft Office	Crítico
Microsoft Office	CVE-2025-53731	Vulnerabilidad de ejecución remota de código de Microsoft Office	Crítico
Microsoft Office Word	CVE-2025-53784	Vulnerabilidad de ejecución remota de código de Microsoft Word	Crítico
Microsoft Office Word	CVE-2025-53733	Vulnerabilidad de ejecución remota de código de Microsoft Word	Crítico
Rol: Windows Hyper-V	CVE-2025-48807	Vulnerabilidad de ejecución remota de código de Windows Hyper-V	Crítico
Windows GDI+	CVE-2025-53766	Vulnerabilidad de ejecución remota de código GDI+	Crítico
Cola de mensajes de Windows	CVE-2025-50177	Vulnerabilidad de ejecución remota de código de Microsoft Message Queue Server (MSMQ)	Crítico

Windows NTLM	CVE-2025-53778	Vulnerabilidad de elevación de privilegios NTLM de Windows	**Crítico**

Vulnerabilidades Altas

Se categorizaron un total de 91 vulnerabilidades con criticidad alta:

Etiqueta	CVE ID	Título	Criticidad
Sincronización de archivos de Azure	CVE-2025-53729	Vulnerabilidad de elevación de privilegios de Microsoft Azure File Sync	Alto
Azure Stack	CVE-2025-53765	Vulnerabilidad de divulgación de información de Azure Stack Hub	Alto
Administrador de Windows de escritorio	CVE-2025-53152	Vulnerabilidad de ejecución remota de código del Administrador de Windows de escritorio	Alto
Administrador de Windows de escritorio	CVE-2025-50153	Vulnerabilidad de elevación de privilegios del Administrador de Windows de escritorio	Alto
GitHub Copilot y Visual Studio	CVE-2025-53773	Vulnerabilidad de ejecución remota de código de GitHub Copilot y Visual Studio	Alto
Controlador de servicio Thunk WOW de transmisión de kernel	CVE-2025-53149	Vulnerabilidad de elevación de privilegios del controlador del servicio WOW Thunk de transmisión de kernel	Alto
Administrador de transacciones del kernel	CVE-2025-53140	Vulnerabilidad de elevación de privilegios del Administrador de transacciones del kernel de Windows	Alto

Sistema de archivos de intermediación de Microsoft	CVE-2025-53142	Vulnerabilidad de elevación de privilegios del sistema de archivos de intermediación de Microsoft	Alto
Microsoft Dynamics 365 (local)	CVE-2025-49745	Vulnerabilidad de scripting entre sitios de Microsoft Dynamics 365 (on-premises)	Alto
Microsoft Dynamics 365 (local)	CVE-2025-53728	Vulnerabilidad de divulgación de información de Microsoft Dynamics 365 (local)	Alto
Servidor de Microsoft Exchange	CVE-2025-25005	Vulnerabilidad de manipulación de Microsoft Exchange Server	Alto
Servidor de Microsoft Exchange	CVE-2025-25006	Vulnerabilidad de suplantación de Microsoft Exchange Server	Alto
Servidor de Microsoft Exchange	CVE-2025-25007	Vulnerabilidad de suplantación de Microsoft Exchange Server	Alto
Servidor de Microsoft Exchange	CVE-2025-53786	Vulnerabilidad de elevación de privilegios de implementación híbrida de Microsoft Exchange Server	Alto
Servidor de Microsoft Exchange	CVE-2025-33051	Vulnerabilidad de divulgación de información de Microsoft Exchange Server	Alto
Componente de gráficos de Microsoft	CVE-2025-49743	Vulnerabilidad de elevación de privilegios del componente de gráficos de Windows	Alto
Microsoft Office	CVE-2025-53732	Vulnerabilidad de ejecución remota de código de Microsoft Office	Alto

Microsoft Office Excel	CVE-2025-53759	Vulnerabilidad de ejecución remota de código de Microsoft Excel	Alto
Microsoft Office Excel	CVE-2025-53737	Vulnerabilidad de ejecución remota de código de Microsoft Excel	Alto
Microsoft Office Excel	CVE-2025-53739	Vulnerabilidad de ejecución remota de código de Microsoft Excel	Alto
Microsoft Office Excel	CVE-2025-53735	Vulnerabilidad de ejecución remota de código de Microsoft Excel	Alto
Microsoft Office Excel	CVE-2025-53741	Vulnerabilidad de ejecución remota de código de Microsoft Excel	Alto
Microsoft Office PowerPoint	CVE-2025-53761	Vulnerabilidad de ejecución remota de código de Microsoft PowerPoint	Alto
Microsoft Office SharePoint	CVE-2025-53760	Vulnerabilidad de elevación de privilegios de Microsoft SharePoint	Alto
Microsoft Office SharePoint	CVE-2025-49712	Vulnerabilidad de ejecución remota de código de Microsoft SharePoint	Alto
Microsoft Office Visio	CVE-2025-53730	Vulnerabilidad de ejecución remota de código de Microsoft Office Visio	Alto
Microsoft Office Visio	CVE-2025-53734	Vulnerabilidad de ejecución remota de código de Microsoft Office Visio	Alto
Microsoft Office Word	CVE-2025-53738	Vulnerabilidad de ejecución remota de código de Microsoft Word	Alto

Microsoft Office Word	CVE-2025-53736	Vulnerabilidad de divulgación de información de Microsoft Word	Alto
Equipos de Microsoft	CVE-2025-53783	Vulnerabilidad de ejecución remota de código de Microsoft Teams	Alto
Protocolo de acceso remoto punto a punto (PPP) EAP-TLS	CVE-2025-50159	Protocolo de punto a punto de acceso remoto (PPP) EAP-TLS Vulnerabilidad de elevación de privilegios	Alto
Servidor de escritorio remoto	CVE-2025-50171	Vulnerabilidad de suplantación de identidad de escritorio remoto	Alto
Rol: Windows Hyper-V	CVE-2025-50167	Vulnerabilidad de elevación de privilegios de Windows Hyper-V	Alto
Rol: Windows Hyper-V	CVE-2025-53155	Vulnerabilidad de elevación de privilegios de Windows Hyper-V	Alto
Rol: Windows Hyper-V	CVE-2025-49751	Vulnerabilidad de denegación de servicio de Windows Hyper-V	Alto
Rol: Windows Hyper-V	CVE-2025-53723	Vulnerabilidad de elevación de privilegios de Windows Hyper-V	Alto
SQL Server	CVE-2025-49758	Vulnerabilidad de elevación de privilegios de Microsoft SQL Server	Alto
SQL Server	CVE-2025-24999	Vulnerabilidad de elevación de privilegios de Microsoft SQL Server	Alto
SQL Server	CVE-2025-53727	Vulnerabilidad de elevación de privilegios de Microsoft SQL Server	Alto

SQL Server	CVE-2025-49759	Vulnerabilidad de elevación de privilegios de Microsoft SQL Server	Alto
SQL Server	CVE-2025-47954	Vulnerabilidad de elevación de privilegios de Microsoft SQL Server	Alto
Controlador de puerto de almacenamiento	CVE-2025-53156	Vulnerabilidad de divulgación de información del controlador del puerto de almacenamiento de Windows	Alto
Implementación web	CVE-2025-53772	Vulnerabilidad de ejecución remota de código de Web Deploy	Alto
Controlador de función auxiliar de Windows para WinSock	CVE-2025-53718	Controlador de función auxiliar de Windows para la vulnerabilidad de elevación de privilegios de WinSock	Alto
Controlador de función auxiliar de Windows para WinSock	CVE-2025-53134	Controlador de función auxiliar de Windows para la vulnerabilidad de elevación de privilegios de WinSock	Alto
Controlador de función auxiliar de Windows para WinSock	CVE-2025-49762	Controlador de función auxiliar de Windows para la vulnerabilidad de elevación de privilegios de WinSock	Alto
Controlador de función auxiliar de Windows para WinSock	CVE-2025-53147	Controlador de función auxiliar de Windows para la vulnerabilidad de elevación de privilegios de WinSock	Alto

Controlador de función auxiliar de Windows para WinSock	CVE-2025-53154	Controlador de función auxiliar de Windows para la vulnerabilidad de elevación de privilegios de WinSock	Alto
Controlador de función auxiliar de Windows para WinSock	CVE-2025-53137	Controlador de función auxiliar de Windows para la vulnerabilidad de elevación de privilegios de WinSock	Alto
Controlador de función auxiliar de Windows para WinSock	CVE-2025-53141	Controlador de función auxiliar de Windows para la vulnerabilidad de elevación de privilegios de WinSock	Alto
Mini controlador de filtro de archivos en la nube de Windows	CVE-2025-50170	Vulnerabilidad de elevación de privilegios del controlador de mini filtro de Windows Cloud Files	Alto
Servicio de plataforma de dispositivos conectados de Windows	CVE-2025-53721	Vulnerabilidad de elevación de privilegios del servicio de plataforma de dispositivos conectados de Windows	Alto
Windows DirectX	CVE-2025-53135	Vulnerabilidad de elevación de privilegios del kernel de gráficos de DirectX	Alto
Windows DirectX	CVE-2025-50172	Vulnerabilidad de denegación de servicio del kernel de gráficos de DirectX	Alto
Coordinador de transacciones distribuidas de Windows	CVE-2025-50166	Vulnerabilidad de divulgación de información del Coordinador de transacciones distribuidas de Windows (MSDTC)	Alto

Explorador de archivos de Windows	CVE-2025-50154	Vulnerabilidad de suplantación de identidad del Explorador de archivos de Microsoft Windows	Alto
Instalador de Windows	CVE-2025-50173	Vulnerabilidad de elevación de privilegios de Windows Installer	Alto
Windows Kernel	CVE-2025-49761	Vulnerabilidad de elevación de privilegios del kernel de Windows	Alto
Windows Kernel	CVE-2025-53151	Vulnerabilidad de elevación de privilegios del kernel de Windows	Alto
Servicio de subsistema de autoridad de seguridad local de Windows (LSASS)	CVE-2025-53716	Vulnerabilidad de denegación de servicio del servicio del subsistema de autoridad de seguridad local (LSASS)	Alto
Windows Media	CVE-2025-53131	Vulnerabilidad de ejecución remota de código de Windows Media	Alto
Cola de mensajes de Windows	CVE-2025-53145	Vulnerabilidad de ejecución remota de código de Microsoft Message Queue Server (MSMQ)	Alto
Cola de mensajes de Windows	CVE-2025-53143	Vulnerabilidad de ejecución remota de código de Microsoft Message Queue Server (MSMQ)	Alto
Cola de mensajes de Windows	CVE-2025-53144	Vulnerabilidad de ejecución remota de código de Microsoft Message Queue Server (MSMQ)	Alto
Kernel del sistema operativo Windows NT	CVE-2025-53136	Vulnerabilidad de divulgación de información del kernel de NT OS	Alto

Windows NTFS	CVE-2025-50158	Vulnerabilidad de divulgación de información NTFS de Windows	Alto
Windows PrintWorkflowUserSvc	CVE-2025-53133	Vulnerabilidad de elevación de privilegios de Windows PrintWorkflowUserSvc	Alto
Notificaciones push de Windows	CVE-2025-53725	Vulnerabilidad de elevación de privilegios de aplicaciones de notificaciones push de Windows	Alto
Notificaciones push de Windows	CVE-2025-53724	Vulnerabilidad de elevación de privilegios de aplicaciones de notificaciones push de Windows	Alto
Notificaciones push de Windows	CVE-2025-50155	Vulnerabilidad de elevación de privilegios de aplicaciones de notificaciones push de Windows	Alto
Notificaciones push de Windows	CVE-2025-53726	Vulnerabilidad de elevación de privilegios de aplicaciones de notificaciones push de Windows	Alto
Servicios de Escritorio remoto de Windows	CVE-2025-53722	Vulnerabilidad de denegación de servicio de los servicios de Escritorio remoto de Windows	Alto
Servicio de enrutamiento y acceso remoto de Windows (RRAS)	CVE-2025-50157	Vulnerabilidad de divulgación de información del servicio de enrutamiento y acceso remoto de Windows (RRAS)	Alto

Servicio de enrutamiento y acceso remoto de Windows (RRAS)	CVE-2025-53153	Vulnerabilidad de divulgación de información del servicio de enrutamiento y acceso remoto de Windows (RRAS)	Alto
Servicio de enrutamiento y acceso remoto de Windows (RRAS)	CVE-2025-50163	Vulnerabilidad de ejecución remota de código del servicio de enrutamiento y acceso remoto de Windows (RRAS)	Alto
Servicio de enrutamiento y acceso remoto de Windows (RRAS)	CVE-2025-50162	Vulnerabilidad de ejecución remota de código del servicio de enrutamiento y acceso remoto de Windows (RRAS)	Alto
Servicio de enrutamiento y acceso remoto de Windows (RRAS)	CVE-2025-50164	Vulnerabilidad de ejecución remota de código del servicio de enrutamiento y acceso remoto de Windows (RRAS)	Alto
Servicio de enrutamiento y acceso remoto de Windows (RRAS)	CVE-2025-53148	Vulnerabilidad de divulgación de información del servicio de enrutamiento y acceso remoto de Windows (RRAS)	Alto
Servicio de enrutamiento y acceso remoto de Windows (RRAS)	CVE-2025-53138	Vulnerabilidad de divulgación de información del servicio de enrutamiento y acceso remoto de Windows (RRAS)	Alto
Servicio de enrutamiento y acceso remoto de Windows (RRAS)	CVE-2025-50156	Vulnerabilidad de divulgación de información del servicio de enrutamiento y acceso remoto de Windows (RRAS)	Alto

Servicio de enrutamiento y acceso remoto de Windows (RRAS)	CVE-2025-49757	Vulnerabilidad de ejecución remota de código del servicio de enrutamiento y acceso remoto de Windows (RRAS)	Alto
Servicio de enrutamiento y acceso remoto de Windows (RRAS)	CVE-2025-53719	Vulnerabilidad de divulgación de información del servicio de enrutamiento y acceso remoto de Windows (RRAS)	Alto
Servicio de enrutamiento y acceso remoto de Windows (RRAS)	CVE-2025-53720	Vulnerabilidad de ejecución remota de código del servicio de enrutamiento y acceso remoto de Windows (RRAS)	Alto
Servicio de enrutamiento y acceso remoto de Windows (RRAS)	CVE-2025-50160	Vulnerabilidad de ejecución remota de código del servicio de enrutamiento y acceso remoto de Windows (RRAS)	Alto
Aplicación de seguridad de Windows	CVE-2025-53769	Vulnerabilidad de suplantación de aplicaciones de seguridad de Windows	Alto
Windows SMB	CVE-2025-50169	Vulnerabilidad de ejecución remota de código SMB de Windows	Alto
Windows StateRepository API	CVE-2025-53789	Vulnerabilidad de elevación de privilegios del archivo del servidor de la API de Windows StateRepository	Alto
Subsistema de Windows para Linux	CVE-2025-53788	Vulnerabilidad de elevación de privilegios del kernel del subsistema de Windows para Linux (WSL2)	Alto

Windows Win32K - GRFX	CVE-2025-50161	Vulnerabilidad de elevación de privilegios de Win32k	Alto
Windows Win32K - GRFX	CVE-2025-53132	Vulnerabilidad de elevación de privilegios de Win32k	Alto
Windows Win32K - ICOMP	CVE-2025-50168	Vulnerabilidad de elevación de privilegios de Win32k	Alto

RECOMENDACIONES

- Prioriza las actualizaciones: No todas las vulnerabilidades son iguales. Utiliza la guía de seguridad de Microsoft para identificar las vulnerabilidades "Críticas" y "Altas" (o "Importantes").
- Evalúa el impacto: Analiza qué sistemas son los más críticos para tu organización y cuáles se verían afectados por las vulnerabilidades más graves.
- Crea un plan de acción: Define quiénes serán los responsables de aplicar los parches, cuándo se realizarán y cómo se comunicarán los cambios.
- Automatiza si es posible: Utiliza herramientas como Microsoft Endpoint Configuration Manager (MECM) o Microsoft Intune para automatizar la implementación de parches.
- Comienza por lo más crítico: Prioriza los parches para las vulnerabilidades "Críticas" y para los sistemas de acceso público, como servidores web o de correo electrónico.
- Verifica la aplicación del parche: Después de la instalación, comprueba que los parches se hayan aplicado correctamente y que los sistemas estén funcionando como se espera.

NOTICIA COMPLETA

https://devel.group/blog/parche-de-microsoft-de-agosto-de-2025-corrige-vulnerabilidad-de-dia-cero-y-108-fallos-de-seguridad/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group