

Alerta ID:	131
Fecha del reporte:	12/08/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades en Patch Tuesday de Microsoft – agosto 2026
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 y herramientas de desarrollo.
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 agosto de 2026**, donde se corrigieron un total de **398** en diferentes productos y componentes del ecosistema Microsoft, incluyendo sistemas operativos Windows, servicios empresariales, aplicaciones de productividad y plataformas utilizadas dentro de la infraestructura tecnológica institucional.

Este documento busca priorizar la mitigación de vulnerabilidades críticas y de día cero, con especial atención a aquellas que puedan afectar la disponibilidad, confidencialidad e integridad de los sistemas que soportan los servicios de salud, fortaleciendo la continuidad operativa y la resiliencia tecnológica de las organizaciones.

Concientizando sobre los riesgos asociados a la explotación de vulnerabilidades, facilitando la identificación de activos, versiones afectadas y controles requeridos,



promoviendo la aplicación oportuna de actualizaciones de seguridad y medidas de mitigación, y fortaleciendo la capacidad de prevención, detección y respuesta ante posibles incidentes de ciberseguridad.

Necesito que me compartas ahora la información base de agosto (cantidad de CVE, vulnerabilidades críticas, zero-days, CVE principales o fuentes), y lo vamos construyendo ítem por ítem con la misma estructura del boletín.

Descripción:



El Martes de Parches (Patch Tuesday) es el ciclo mensual de actualizaciones de seguridad publicado por Microsoft el segundo martes de cada mes. Este mecanismo, establecido desde octubre de 2003, centraliza la distribución de correcciones de seguridad, actualizaciones críticas y mejoras funcionales para todo el ecosistema de productos Microsoft, incluyendo sistemas operativos Windows, Microsoft Office, SharePoint, Active Directory, .NET, Azure, servicios empresariales y herramientas de desarrollo.

El ciclo de **Patch Tuesday de agosto de 2026**, publicado el **11 de agosto de 2026**, incluye actualizaciones de seguridad orientadas a corregir vulnerabilidades identificadas en diferentes componentes del ecosistema Microsoft. Estas correcciones buscan reducir la superficie de ataque, fortalecer los controles de seguridad y mitigar riesgos asociados a posibles escenarios de explotación contra estaciones de trabajo, servidores y plataformas utilizadas por las organizaciones.

A continuación, se presenta el resumen estadístico:

Categoría	Cantidad
Total de vulnerabilidades corregidas	398 CVEs
Vulnerabilidades Críticas	44



Categoría	Cantidad
Vulnerabilidades Importantes	354
Moderadas / Bajas	No reportadas como categoría independiente
Día cero explotado activamente	1(CVE-2026-68820)
Día cero divulgado públicamente	1 (CVE-2026-62832)
RCE Críticas	No especificado en el resumen inicial
DoS Críticas	No especificado en el resumen inicial

Las familias de productos afectados incluyen: Windows Boot Loader, Windows Kernel, Windows Active Directory, Windows IKE Extension, Windows TCP/IP, Microsoft Office (Word, Excel, PowerPoint), Microsoft SharePoint, Remote Desktop Client, .NET Framework, Microsoft Defender, Windows BitLocker, Hyper-V, Azure Logic Apps, SQL Server, Windows Hello, Windows Kerberos, entre otros.

Distribución de Vulnerabilidades

Con respecto al total de las vulnerabilidades reportadas por Microsoft se encuentran categorizadas de la siguiente manera según el tipo:

Omisión de funciones de seguridad: 11

Spoofing: 21

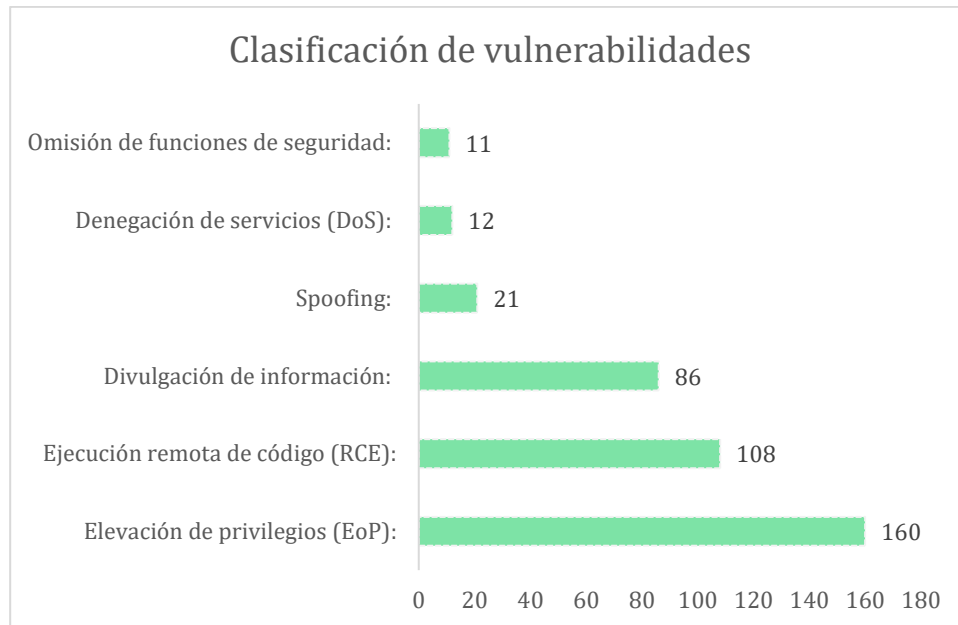
Denegación de servicios (DoS): 12

Ejecución remota de código (RCE): 108

Divulgación de información: 86

Elevación de privilegios (EoP): 160





Las vulnerabilidades de elevación de privilegios (EoP) representan la categoría con mayor número de fallas identificadas durante este ciclo de actualización, con 160 vulnerabilidades corregidas. Estas vulnerabilidades representan un riesgo significativo debido a que pueden permitir que un atacante con acceso inicial al sistema aumente sus permisos dentro del entorno tecnológico, alcanzando niveles administrativos y comprometiendo recursos críticos de la organización.

Por otra parte, las vulnerabilidades de ejecución remota de código (RCE), con 110 casos reportados, requieren una atención prioritaria debido a que pueden permitir la ejecución de instrucciones no autorizadas en sistemas afectados, comprometiendo servidores, estaciones de trabajo y aplicaciones críticas utilizadas por las entidades.

Para las organizaciones del sector salud, las categorías con mayor impacto operativo corresponden principalmente a:



- Elevación de privilegios (EoP): debido al alto número de vulnerabilidades identificadas en esta categoría, las cuales pueden permitir que un atacante con acceso inicial a un sistema incremente sus permisos, obtenga privilegios administrativos y comprometa recursos críticos dentro de la infraestructura tecnológica institucional.
- Ejecución remota de código (RCE): debido al riesgo de ejecución de instrucciones no autorizadas en servidores, estaciones clínicas, sistemas administrativos y plataformas críticas, pudiendo generar compromisos completos de activos tecnológicos utilizados para la prestación de servicios de salud.
- Divulgación de información: debido a la posibilidad de exposición de datos sensibles almacenados en sistemas institucionales, incluyendo información de pacientes, registros administrativos, configuraciones internas y credenciales utilizadas por plataformas tecnológicas.
- Spoofing y omisión de funciones de seguridad: debido a la posibilidad de que un atacante suplante identidades, evada mecanismos de protección establecidos o reduzca la efectividad de controles de seguridad implementados en soluciones Microsoft.

La aplicación prioritaria de los parches asociados a estas categorías, especialmente en activos expuestos a internet, servidores institucionales, controladores de dominio, plataformas de colaboración, sistemas que gestionan información clínica y equipos utilizados por usuarios con privilegios elevados, resulta fundamental para reducir la superficie de ataque, prevenir accesos no autorizados y fortalecer la resiliencia tecnológica de las organizaciones del sector salud.

Vulnerabilidades de Día Cero y Más Importantes

Este ciclo de actualización incluye **dos vulnerabilidades clasificadas como día cero**, una de ellas **explotada activamente en escenarios reales** y otra **divulgada públicamente antes de la disponibilidad del parche**. Adicionalmente, el ciclo de agosto de 2026 incluye vulnerabilidades críticas de alta relevancia para las organizaciones del sector salud, especialmente aquellas



relacionadas con elevación de privilegios, ejecución remota de código y componentes esenciales del sistema operativo Windows.

A continuación, se presentan las vulnerabilidades de día cero:

CVE-2026-68820 — Windows AFD Driver: Vulnerabilidad de Elevación de Privilegios (Explotada Activamente).

CVE	CVE-2026-68820
CVSS v3	7.0 (Importante, explotado activamente)
Tipo	Elevación de privilegios (EoP) / Use-After-Free
Producto afectado	Windows Ancillary Function Driver for WinSock (afd.sys)
Estado	EXPLOTADO ACTIVAMENTE
Impacto principal	Escalada de privilegios hasta nivel SYSTEM

Esta vulnerabilidad afecta al controlador AFD (Ancillary Function Driver for WinSock) utilizado por Windows para la gestión de comunicaciones de red. La falla de tipo use-after-free puede ser aprovechada por un atacante con acceso local al sistema para ejecutar código con privilegios elevados hasta alcanzar el nivel SYSTEM, comprometiendo completamente el equipo afectado.

Aunque requiere acceso inicial al sistema, su explotación representa un riesgo significativo debido a que permite la escalada de privilegios posterior a una intrusión, facilitando acciones como deshabilitar controles de seguridad, instalar herramientas maliciosas, ejecutar movimientos laterales y comprometer otros activos dentro de la organización.



Para entidades del sector salud, esta vulnerabilidad representa un riesgo relevante en estaciones clínicas, equipos administrativos y servidores Windows utilizados para soportar servicios institucionales

CVE-2026-62832 — Windows User Profile Service: Vulnerabilidad de Elevación de Privilegios (Divulgada Públicamente)

CVE	CVE-2026-62832
CVSS v3	7.8 (Importante)
Tipo	Elevación de privilegios (EoP)
Producto afectado	Windows User Profile Service
Estado	DIVULGADO PÚBLICAMENTE
Explotación pública	Información disponible antes del parche

Esta vulnerabilidad afecta al servicio de perfiles de usuario de Windows y puede permitir que un atacante autenticado con una cuenta local obtenga privilegios superiores mediante la manipulación de recursos asociados al perfil del usuario y acceso no autorizado a componentes del sistema.

La divulgación pública previa a la disponibilidad del parche incrementa el riesgo de explotación, especialmente en ambientes donde existen equipos compartidos, estaciones administrativas, servidores de acceso remoto o dispositivos utilizados por múltiples usuarios.

En escenarios del sector salud, podría facilitar la escalada desde cuentas con permisos limitados hacia niveles administrativos, permitiendo acceso no autorizado a aplicaciones institucionales, información sensible o recursos internos.



Vulnerabilidades Críticas Adicionales de Alta Relevancia.

CVE	CVSS	Tipo	Descripción resumida
CVE-2026-68820	7.0	EoP	Windows Ancillary Function Driver (AFD) — Vulnerabilidad de elevación de privilegios mediante condición de uso después de liberación (Use-After-Free), permitiendo a un atacante local obtener privilegios SYSTEM. Explotada activamente.
CVE-2026-62832	7.8	EoP	Windows User Profile Service — Vulnerabilidad de elevación de privilegios divulgada públicamente que puede permitir a un atacante autenticado obtener permisos superiores dentro del sistema operativo.
Pendiente validación MSRC	Crítico	RCE/EoP	Windows — Vulnerabilidad de ejecución remota de código con potencial impacto sobre sistemas expuestos y servicios críticos del ecosistema Microsoft.
Pendiente validación MSRC	Crítico	RCE	Microsoft Office / Windows — Vulnerabilidad de ejecución remota de código mediante archivos manipulados, con riesgo de explotación mediante campañas de phishing dirigidas.
Pendiente validación MSRC	Crítico	Seguridad Microsoft	Servicios Windows — Vulnerabilidad que permite ejecución de código no autorizado mediante solicitudes especialmente diseñadas.

Consecuencias de la Explotación

La explotación exitosa de las vulnerabilidades descritas en este boletín puede generar consecuencias de alto impacto para las entidades del sector salud, incluyendo:

Escalada de Privilegios hasta nivel SYSTEM (CVE-2026-68820 — Windows AFD Driver)



- Un atacante con acceso inicial al sistema puede aprovechar la vulnerabilidad para incrementar sus privilegios locales hasta obtener permisos SYSTEM dentro del sistema operativo.
- Permite evadir restricciones de seguridad implementadas en el equipo afectado, facilitando la ejecución de procesos con privilegios elevados.
- Puede ser utilizada como una etapa posterior a una intrusión inicial para instalar malware persistente, herramientas de acceso remoto no autorizado (RAT) o mecanismos de permanencia dentro de la infraestructura.
- En ambientes de salud podría facilitar el compromiso de estaciones clínicas, equipos administrativos y servidores Windows utilizados para soportar servicios institucionales.

Compromiso de cuentas y recursos internos mediante Elevación de Privilegios (CVE-2026-62832 — Windows User Profile Service)

- Un atacante autenticado con permisos limitados podría obtener privilegios superiores dentro del sistema afectado.
- La escalada de permisos puede permitir acceso a configuraciones sensibles, servicios internos y recursos restringidos de la organización.
- Puede facilitar movimientos laterales hacia otros activos tecnológicos, especialmente en entornos con autenticación centralizada mediante Active Directory.
- En entidades del sector salud podría generar acceso no autorizado a aplicaciones institucionales, sistemas administrativos y plataformas que gestionan información sensible.

Ejecución Remota de Código en componentes críticos de Microsoft



- Las vulnerabilidades críticas de ejecución remota de código pueden permitir que un atacante ejecute instrucciones no autorizadas sobre sistemas afectados mediante solicitudes especialmente diseñadas.
- Un compromiso exitoso puede afectar servidores, estaciones de trabajo y servicios esenciales utilizados para la operación institucional.
- En redes hospitalarias puede facilitar movimientos laterales hacia sistemas críticos como plataformas HIS, RIS, PACS, bases de datos clínicas y servicios de soporte tecnológico.
- Existe riesgo de despliegue de ransomware, interrupción de servicios tecnológicos y afectación de la continuidad operativa.

Compromiso de información institucional y datos sensibles

- Las vulnerabilidades asociadas a divulgación de información pueden permitir el acceso no autorizado a datos almacenados en sistemas Microsoft.
- La exposición puede involucrar información clínica, datos personales de pacientes, documentación administrativa, configuraciones internas y credenciales utilizadas por aplicaciones institucionales.
- La información obtenida podría ser utilizada para ataques posteriores como phishing dirigido, fraude, suplantación de identidad o accesos no autorizados.

Afectación mediante componentes Microsoft Office y documentos maliciosos



- Las vulnerabilidades presentes en aplicaciones de productividad pueden ser aprovechadas mediante archivos Office manipulados enviados por correo electrónico u otros medios de comunicación.
- Representan un vector frecuente de ataque contra usuarios administrativos y personal asistencial mediante campañas de phishing dirigidas.

La apertura de documentos maliciosos podría permitir la ejecución de código no autorizado, descarga de malware y compromiso del equipo del usuario..

Modo de Explotación de las vulnerabilidades de day-zero y críticas.

Explotación de CVE-2026-68820 (Windows AFD Driver — Elevación de Privilegios — Explotada Activamente)

Acceso inicial:

El atacante requiere contar previamente con acceso al sistema objetivo mediante una cuenta local, credenciales comprometidas, explotación de otra vulnerabilidad o mecanismos de acceso no autorizado. La vulnerabilidad no permite el acceso inicial remoto por sí sola, sino que funciona como una etapa posterior para aumentar privilegios dentro del equipo comprometido.

Explotación:

El atacante aprovecha una condición de tipo **Use-After-Free** en el controlador **Ancillary Function Driver for WinSock (afd.sys)** de Windows, manipulando la gestión de memoria del componente para ejecutar código con permisos elevados. Mediante esta técnica, puede obtener privilegios del nivel **SYSTEM**, superando las restricciones establecidas para usuarios con permisos limitados.

Escalada de privilegios:



Una vez obtenido el contexto SYSTEM, el atacante puede ejecutar procesos con privilegios máximos, modificar configuraciones de seguridad, acceder a información restringida y deshabilitar mecanismos de protección instalados en el sistema operativo.

Post-explotación:

Con privilegios elevados, el atacante puede establecer persistencia mediante creación de usuarios privilegiados, modificación de configuraciones del sistema, instalación de herramientas de acceso remoto no autorizado y realizar movimientos laterales hacia otros equipos dentro de la infraestructura institucional.

- **Explotación de CVE-2026-62832 (Windows User Profile Service — Elevación de Privilegios — Divulgada Públicamente)**

Acceso inicial:

El atacante obtiene una cuenta válida con privilegios limitados dentro del sistema operativo mediante phishing, credenciales comprometidas, acceso físico o explotación previa de otro componente vulnerable.

Manipulación del servicio:

El atacante aprovecha una debilidad en el servicio de perfiles de usuario de Windows para interactuar con componentes internos del sistema y realizar acciones no autorizadas sobre recursos protegidos.

Escalada de privilegios:

La explotación permite incrementar los permisos de la cuenta comprometida, pasando de un usuario con privilegios reducidos a un contexto con mayores capacidades dentro del sistema operativo.

Persistencia y movimiento lateral:

Con mayores privilegios, el atacante puede acceder a recursos adicionales, modificar configuraciones locales, comprometer aplicaciones institucionales y utilizar el equipo afectado como punto de entrada hacia otros activos de la organización.

- **Explotación de vulnerabilidades críticas de Ejecución Remota de Código (RCE) en componentes Microsoft Windows**

Identificación de objetivos:

El atacante realiza reconocimiento sobre sistemas Windows expuestos o accesibles dentro de la red institucional, identificando versiones vulnerables, servicios activos y componentes Microsoft sin actualizar.

Construcción de solicitudes maliciosas:

Se generan solicitudes o datos especialmente diseñados para aprovechar errores en componentes vulnerables del sistema operativo o servicios Microsoft, buscando ejecutar instrucciones no autorizadas dentro del equipo objetivo.

Ejecución de código:

Cuando el componente vulnerable procesa la solicitud manipulada, el atacante puede ejecutar código con los privilegios del servicio afectado, permitiendo la instalación de cargas maliciosas, modificación del sistema o acceso no autorizado a recursos internos.

Post-explotación:

Después del compromiso inicial, el atacante puede realizar reconocimiento interno, extracción de información, movimiento lateral hacia servidores críticos y afectar sistemas utilizados para la operación institucional.

- **Explotación de vulnerabilidades Microsoft Office — RCE mediante documentos maliciosos**

Preparación del documento:



El atacante crea archivos Office manipulados, como documentos Word, Excel u otros formatos compatibles, diseñados para aprovechar vulnerabilidades presentes en componentes de procesamiento de archivos Microsoft.

Entrega:

El archivo malicioso puede ser distribuido mediante campañas de phishing, correos electrónicos dirigidos, plataformas de mensajería institucional o sitios web comprometidos. En el sector salud, estos mensajes pueden simular comunicaciones relacionadas con resultados médicos, proveedores, entidades regulatorias o procesos administrativos.

Ejecución:

Cuando el usuario abre el documento utilizando una versión vulnerable de Microsoft Office, el componente afectado procesa el contenido manipulado y puede permitir la ejecución de código no autorizado en el equipo del usuario.

Post-explotación:

El atacante puede descargar herramientas adicionales, capturar información, establecer persistencia y utilizar el equipo comprometido como punto de entrada para ataques posteriores contra la infraestructura tecnológica institucional.

Recursos y versiones afectadas:

- **Sistemas Operativos Windows**

Sistema Operativo	Versiones / Builds Afectadas
Windows 11	Versiones 23H2, 24H2 y 25H2 con actualizaciones acumulativas anteriores al parche de seguridad de agosto de 2026.
Windows 10	Versión 22H2 con actualizaciones acumulativas anteriores al parche de seguridad de agosto de 2026.



Sistema Operativo	Versiones / Builds Afectadas
Windows Server 2025	Versiones RTM y actualizaciones acumulativas anteriores a agosto de 2026.
Windows Server 2022	Versiones anteriores a las actualizaciones acumulativas de seguridad de agosto de 2026.
Windows Server 2019	Versiones anteriores a las actualizaciones acumulativas de seguridad de agosto de 2026.
Windows Server 2016	Versiones anteriores a las actualizaciones acumulativas de seguridad de agosto de 2026.

- **Aplicaciones y Servicios Microsoft**

Producto / Componente	Versiones Afectadas
Microsoft Office (Word, Excel, PowerPoint)	Office 2016, Office 2019, Office LTSC 2021, Office LTSC 2024 y Microsoft 365 Apps para empresas con actualizaciones anteriores a agosto de 2026.
Microsoft Defender	Versiones de plataforma, motor y definiciones anteriores a las actualizaciones de seguridad de agosto de 2026.
Windows Active Directory Domain Services (AD DS)	Implementaciones en Windows Server 2016, 2019, 2022 y 2025 sin las actualizaciones acumulativas de agosto de 2026.
Remote Desktop Services / Remote Desktop Client	Componentes RDP integrados en Windows 10, Windows 11 y Windows Server sin actualización de seguridad aplicada.
.NET Framework	Versiones .NET Framework 3.5, 4.6.2, 4.7.x, 4.8 y 4.8.1 anteriores a los parches de agosto de 2026.



Producto / Componente	Versiones Afectadas
Windows Kernel y componentes del sistema	Componentes del núcleo Windows afectados por vulnerabilidades de elevación de privilegios y ejecución remota de código corregidas en agosto de 2026.
Windows Networking Components	Componentes de red de Windows, incluyendo controladores y servicios relacionados con comunicaciones del sistema operativo.
Microsoft SQL Server	Versiones SQL Server 2019, SQL Server 2022 y ediciones compatibles sin las actualizaciones de seguridad correspondientes.
Microsoft Edge (Chromium)	Versiones anteriores a las actualizaciones de seguridad liberadas durante agosto de 2026.
Azure y servicios empresariales Microsoft	Componentes y agentes con actualizaciones de seguridad pendientes correspondientes al ciclo de agosto de 2026.

Vector de impacto:



- **Elevación de Privilegios (EoP)**

Este fue el vector de impacto predominante durante el ciclo de actualización de agosto de 2026, con aproximadamente 176 vulnerabilidades identificadas.

Las vulnerabilidades de elevación de privilegios permiten que un atacante con acceso inicial al sistema aumente sus permisos dentro del entorno tecnológico, pudiendo obtener privilegios administrativos o nivel SYSTEM. Este tipo de vulnerabilidades suelen ser utilizadas como una segunda fase después de una intrusión inicial para ampliar el control sobre equipos comprometidos, deshabilitar controles de seguridad y acceder a recursos restringidos.

- **Ejecución Remota de Código (RCE)**



Durante este ciclo se identificaron aproximadamente 110 vulnerabilidades relacionadas con ejecución remota de código.

Las vulnerabilidades RCE representan uno de los mayores riesgos para las organizaciones debido a que pueden permitir la ejecución de instrucciones no autorizadas sobre sistemas afectados mediante solicitudes o archivos especialmente diseñados. Una explotación exitosa puede generar compromiso completo de servidores, estaciones de trabajo y aplicaciones críticas utilizadas en ambientes institucionales.

● **Divulgación de Información**

Se identificaron aproximadamente 86 vulnerabilidades asociadas a divulgación de información.

Estas fallas pueden permitir el acceso no autorizado a información que debería permanecer protegida, incluyendo configuraciones internas, datos almacenados en sistemas Microsoft, credenciales, información de usuarios y otros elementos que pueden ser utilizados para ataques posteriores.

En entidades del sector salud representan un riesgo relevante debido al posible impacto sobre información clínica, datos personales de pacientes y documentación administrativa.

● **Suplantación de Identidad (Spoofing)**

Se corrigieron aproximadamente 21 vulnerabilidades relacionadas con Spoofing.

Estas vulnerabilidades pueden permitir que un atacante suplante la identidad de usuarios, servicios o componentes tecnológicos, afectando la confianza de los sistemas y facilitando ataques dirigidos contra usuarios internos o plataformas institucionales.

● **Denegación de Servicio (DoS)**

Se identificaron aproximadamente 12 vulnerabilidades de Denegación de Servicio.



Estas vulnerabilidades pueden afectar la disponibilidad de servicios tecnológicos al provocar fallas, interrupciones o degradación del rendimiento de componentes afectados, generando posibles impactos sobre sistemas utilizados para la operación institucional.

- **Omisión de funciones de seguridad**

Se corrigieron aproximadamente 11 vulnerabilidades asociadas a omisión de controles de seguridad.

Estas fallas pueden permitir que un atacante evada mecanismos de protección implementados en productos Microsoft, reduciendo la efectividad de controles diseñados para proteger sistemas, usuarios y datos institucionales.

Recomendaciones de mitigación:

Las siguientes acciones deben ejecutarse de forma transversal en todos los sistemas afectados:

Aplicar las actualizaciones de seguridad de agosto de 2026 de Microsoft mediante Windows Update, WSUS, SCCM o Microsoft Intune para todos los sistemas Windows identificados dentro del inventario tecnológico institucional.

Priorizar la aplicación de parches sobre vulnerabilidades de alta criticidad, especialmente aquellas asociadas a:

CVE-2026-68820 — Windows AFD Driver (Elevación de Privilegios, explotada activamente).

CVE-2026-62832 — Windows User Profile Service (Elevación de Privilegios, divulgada públicamente).

Vulnerabilidades críticas de ejecución remota de código (RCE) identificadas durante el ciclo de actualización de agosto de 2026.

Validar y actualizar los sistemas operativos Windows Server y estaciones de trabajo, priorizando:

Controladores de dominio.



Servidores de aplicaciones.

Servidores de bases de datos.

Equipos utilizados por usuarios administrativos.

Equipos asociados a servicios clínicos y administrativos.

Mantener actualizadas las plataformas de seguridad Microsoft Defender, incluyendo motor, plataforma y definiciones de inteligencia de seguridad, con el objetivo de reducir riesgos asociados a vulnerabilidades de elevación de privilegios y técnicas de evasión de controles.

Aplicar las actualizaciones correspondientes de Microsoft Office en todas las estaciones de trabajo institucionales, especialmente aquellas utilizadas para procesamiento de documentos, correo electrónico y gestión administrativa, reduciendo el riesgo asociado a archivos maliciosos y campañas de phishing.

Verificar la aplicación de actualizaciones en servicios críticos de autenticación, incluyendo Active Directory Domain Services, servidores Windows y componentes relacionados con gestión de identidades.

Realizar validaciones posteriores al parcheo, verificando:

Correcta instalación de actualizaciones.

Reinicio de servicios requeridos.

Estado operativo de aplicaciones críticas.

Integridad de sistemas clínicos y administrativos.

Mitigaciones Adicionales y Hardening

- **Implementar el principio de mínimo privilegio:** asegurar que usuarios clínicos, administrativos y operativos trabajen con cuentas estándar, evitando privilegios de administrador local que puedan facilitar escaladas de privilegios.
- **Revisar y fortalecer las políticas de Active Directory:** aplicar controles sobre cuentas privilegiadas, grupos administrativos, políticas de contraseña, autenticación multifactor y permisos asignados.



- **Implementar segmentación de red y controles de acceso:** limitar la comunicación entre segmentos administrativos, clínicos y servidores críticos para reducir movimientos laterales en caso de compromiso.
- **Mantener habilitados mecanismos de protección de endpoint:** verificar que Microsoft Defender, soluciones EDR y controles antimalware permanezcan activos y actualizados en todos los equipos del parque tecnológico.
- **Fortalecer la seguridad del correo electrónico institucional:** configurar filtros para identificar y bloquear archivos potencialmente maliciosos como documentos Office manipulados, archivos ejecutables y enlaces sospechosos provenientes de fuentes externas.
- **Activar mecanismos de protección en Microsoft Office:** mantener habilitada la vista protegida (Protected View), bloqueo de macros no confiables y controles adicionales para documentos descargados desde Internet.
- **Realizar monitoreo continuo de eventos de seguridad:** revisar registros de Windows, eventos de autenticación, creación de usuarios privilegiados, cambios de configuración y comportamientos anómalos posteriores a la aplicación de parches.
- **Implementar controles de respaldo y recuperación:** verificar que los respaldos de sistemas críticos se encuentren actualizados, protegidos y disponibles ante posibles escenarios de ransomware o compromiso de infraestructura.
- **Mantener una gestión periódica de vulnerabilidades:** establecer ciclos de identificación, priorización, actualización y validación de parches para reducir la exposición de activos tecnológicos institucionales.

Fuentes:



- Microsoft Security Response Center (MSRC) — Guía de actualizaciones de agosto 2026:
<https://msrc.microsoft.com/update-guide>
- CISA Known Exploited Vulnerabilities Catalog — Vulnerabilidades Microsoft agosto 2026:
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



- Qualys — Microsoft and Adobe Patch Tuesday, August 2026 Security Update Review
- Tenable — Microsoft August 2026 Patch Tuesday Security Updates
- Cisco Talos Intelligence — Microsoft Patch Tuesday for August 2026: Snort Rules and Prominent Vulnerabilities
- Lansweeper — Microsoft Patch Tuesday August 2026
- BleepingComputer — Microsoft August 2026 Patch Tuesday Security Updates
- MITRE ATT&CK Framework v15:
<https://attack.mitre.org>
- Microsoft Security Update Guide — August 2026 Cumulative Updates for Windows

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.

