

Alerta ID:	124
Fecha del reporte:	15/07/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades en Patch Tuesday de Microsoft – Julio 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 organizaciones del sector salud en Colombia sobre las vulnerabilidades de seguridad abordadas durante el **Patch Tuesday de Microsoft de julio de 2026**, el cual incluye **570 vulnerabilidades** abordadas y múltiples fallas críticas, incluyendo vulnerabilidades de día cero explotadas activamente, incluyendo sistemas operativos Windows, servicios empresariales, plataformas de administración y componentes utilizados en infraestructuras tecnológicas institucionales.

El propósito de esta alerta es priorizar la identificación y mitigación de vulnerabilidades críticas, de alta severidad y aquellas con evidencia de explotación activa, con el fin de reducir riesgos que puedan afectar la continuidad operativa de los servicios tecnológicos que soportan los procesos asistenciales, administrativos y de gestión de información en las entidades del sector salud.



Esta comunicación busca fortalecer la capacidad de las organizaciones para identificar activos tecnológicos afectados, validar versiones de software implementadas, aplicar actualizaciones de seguridad de manera oportuna y ejecutar medidas preventivas que permitan proteger servidores, estaciones de trabajo, servicios en la nube y componentes críticos de infraestructura frente a posibles vectores de ataque.

Adicionalmente, se busca promover la adopción de buenas prácticas de gestión de vulnerabilidades, monitoreo continuo, fortalecimiento de controles de seguridad y preparación ante incidentes cibernéticos, contribuyendo a garantizar la confidencialidad, integridad y disponibilidad de la información clínica y administrativa, así como la resiliencia tecnológica necesaria para la continuidad de los servicios de salud.

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 Framework, servicios en la nube Azure y diferentes herramientas utilizadas en ambientes empresariales.

El ciclo de **Patch Tuesday de julio de 2026**, publicado el **14 de julio de 2026**, incluye correcciones de seguridad dirigidas a múltiples productos y componentes del ecosistema Microsoft. Estas actualizaciones tienen como objetivo mitigar vulnerabilidades que pueden afectar sistemas operativos, servicios empresariales, plataformas de administración, herramientas de productividad y componentes críticos utilizados por organizaciones públicas y privadas.

Para las organizaciones del sector salud, este ciclo de actualización representa una actividad prioritaria debido a la dependencia tecnológica de productos Microsoft en servidores



institucionales, estaciones de trabajo clínicas y administrativas, plataformas de autenticación, sistemas de gestión documental, servicios de comunicación y aplicaciones integradas con procesos misionales.

A continuación, se presenta el resumen estadístico del ciclo de actualización:

Categoría	Cantidad
Total, de vulnerabilidades corregidas	570 CVEs
Vulnerabilidades Críticas	61
Vulnerabilidades Importantes	509
Moderadas / Bajas	No reportadas
Día cero explotado activamente	3 CVE-2026-50661 CVE-2026-56155 CVE-2026-56164
Día cero divulgado públicamente	Por confirmar en MSRC
RCE Críticas	Incluidas dentro del conjunto total de vulnerabilidades corregidas
DoS Críticas	Incluidas dentro del conjunto total de vulnerabilidades corregidas

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: 17

Spoofing: 16

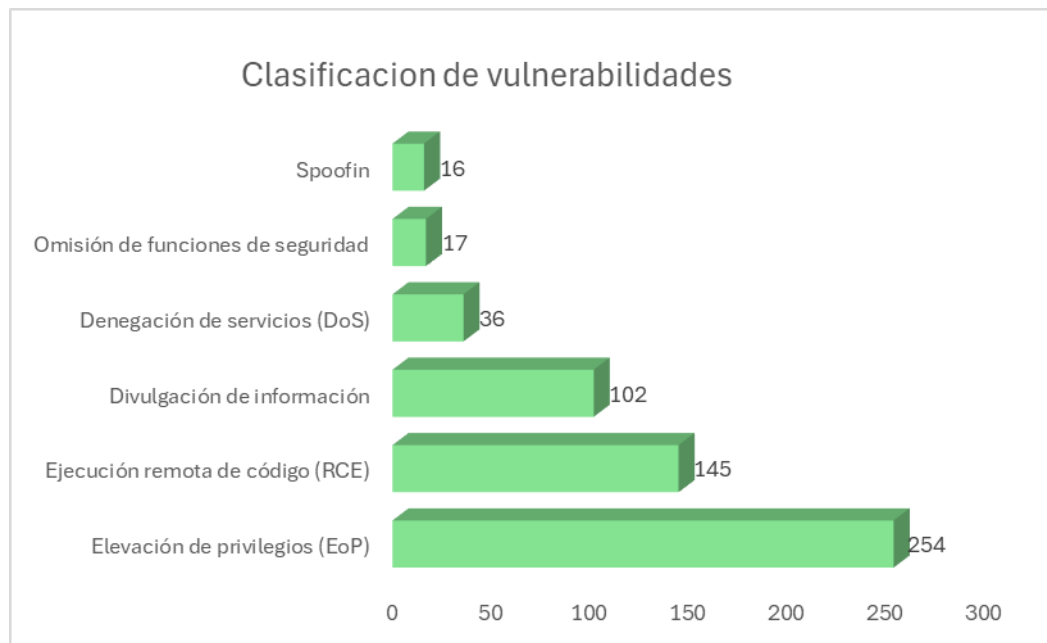
Denegación de servicios (DoS): 36

Ejecución remota de código (RCE): 145

Divulgación de información: 102

Elevación de privilegios (EoP): 254

Total, de vulnerabilidades categorizadas 570



Las vulnerabilidades de elevación de privilegios (EoP) representan la mayor proporción del ciclo de actualización, con 254 fallas identificadas, lo que evidencia un riesgo significativo



asociado a escenarios donde un atacante con acceso inicial podría aumentar sus permisos dentro de sistemas Windows o servicios Microsoft.

Por otra parte, las vulnerabilidades clasificadas como ejecución remota de código (RCE), con 145 casos reportados, requieren una atención prioritaria debido a que pueden permitir la ejecución de instrucciones no autorizadas en servidores o estaciones de trabajo afectadas, comprometiendo potencialmente aplicaciones, servicios y activos críticos de las organizaciones.

Las vulnerabilidades de divulgación de información, con 102 casos, también representan un riesgo relevante para entidades del sector salud, debido a la posibilidad de exposición de información almacenada en sistemas institucionales, configuraciones internas, credenciales u otros datos utilizados por plataformas tecnológicas.

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

- Ejecución remota de código (RCE): debido al riesgo de compromiso directo de servidores, estaciones clínicas, sistemas administrativos y plataformas críticas.
- Elevación de privilegios (EoP): por la posibilidad de que un atacante amplíe sus permisos dentro del entorno tecnológico y acceda a recursos restringidos.
- Divulgación de información: debido al manejo de datos sensibles asociados a pacientes, procesos administrativos y operación institucional.
- Omisión de controles de seguridad: por la posibilidad de evadir mecanismos de protección implementados en sistemas 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 y equipos utilizados por usuarios con privilegios elevados, es fundamental para reducir la superficie de ataque 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 explotada activamente en la naturaleza y otra divulgada públicamente antes de la disponibilidad del parche. Adicionalmente, se identificaron ocho vulnerabilidades Críticas de alta relevancia para el sector.

A continuación, se presentan las vulnerabilidades de día zero.

- **CVE-2026-32201 — Microsoft SharePoint Server: Vulnerabilidad de Suplantación (Explotada Activamente)**

CVE	CVE-2026-32201
CVSS v3	6.5 (Importante — explotado activamente)
Tipo	Spoofing / Validación incorrecta de entradas
Producto afectado	Microsoft Office SharePoint Server
Estado	EXPLOTADO ACTIVAMENTE — Listado en CISA KEV
Fecha límite CISA	28 de abril de 2026

Esta vulnerabilidad, causada por una validación incorrecta de entradas (Improper Input Validation) en Microsoft Office SharePoint, permite a un atacante no autenticado ejecutar ataques de suplantación (spoofing) a través de la red sin requerir interacción del usuario. Un



atacante que explote esta falla puede visualizar información sensible y realizar modificaciones sobre la información divulgada, afectando la Confidencialidad e Integridad del sistema, aunque sin impacto directo sobre la Disponibilidad.

Microsoft no ha divulgado el método específico de explotación ni el actor de amenaza responsable. El crédito de descubrimiento tampoco fue atribuido públicamente. Su inclusión en el catálogo KEV de CISA confirma que actores maliciosos la están utilizando en ataques reales.

- **CVE-2026-33825 — Microsoft Defender: Elevación de Privilegios (Divulgado Públicamente — BlueHammer)**

CVE	CVE-2026-50661
CVSS v3	7.8 (Importante)
Tipo	Elevación de privilegios (Elevation of Privilege - EoP)
Producto afectado	Componentes del sistema operativo Windows
Estado	EXPLOTADO ACTIVAMENTE — Priorización inmediata)
Exploit público	Confirmada en escenarios reales

Esta vulnerabilidad permite que un atacante con acceso inicial a un sistema Windows pueda ejecutar acciones con privilegios superiores a los autorizados, aprovechando una debilidad en los mecanismos internos de control de permisos del sistema operativo.



La explotación exitosa podría permitir a un atacante pasar desde un contexto de usuario limitado hacia niveles elevados de privilegio, incluyendo capacidades administrativas, comprometiendo controles de seguridad establecidos y aumentando la posibilidad de afectar otros recursos dentro del entorno corporativo.

Para las organizaciones del sector salud, esta vulnerabilidad representa un riesgo relevante debido a que estaciones de trabajo clínicas, administrativas y servidores Windows suelen manejar accesos a aplicaciones críticas, sistemas institucionales, plataformas de gestión documental y recursos compartidos.

Microsoft no ha divulgado públicamente detalles completos del método utilizado para explotar esta vulnerabilidad ni información específica sobre los actores responsables. Su clasificación como vulnerabilidad explotada activamente indica que debe ser tratada como una prioridad dentro de los procesos de gestión de parches.

CVE-2026-56155 — Vulnerabilidad de Ejecución Remota de Código en Windows (Explotada Activamente)

CVE	CVE-2026-56155
CVSS v3	Crítico / Alto impacto
Tipo	Ejecución remota de código (Remote Code Execution - RCE)
Producto afectado	Componentes Microsoft Windows
Estado	EXPLOTADO ACTIVAMENTE
Impacto principal	Compromiso remoto de sistemas afectados



Esta vulnerabilidad permite que un atacante pueda ejecutar código no autorizado en un sistema afectado mediante la explotación de una condición vulnerable en componentes de Windows expuestos a determinadas solicitudes o interacciones maliciosas.

Un atacante que aproveche esta falla podría ejecutar instrucciones dentro del sistema comprometido, instalar software malicioso, modificar configuraciones, acceder a información sensible o utilizar el equipo como punto inicial para ataques posteriores dentro de la infraestructura tecnológica.

En ambientes de salud, una explotación exitosa podría afectar servidores institucionales, estaciones utilizadas por personal asistencial, sistemas administrativos y equipos integrados con plataformas críticas, generando riesgos sobre la continuidad de los servicios tecnológicos.

La explotación activa de esta vulnerabilidad incrementa la probabilidad de ataques dirigidos contra organizaciones que mantengan sistemas sin actualizar, especialmente aquellas con servicios expuestos a internet o con infraestructura Microsoft ampliamente implementada.

CVE-2026-56164 — Vulnerabilidad Crítica en Servicios Microsoft (Explotada Activamente)

CVE	CVE-2026-56164
CVSS v3	Alta / Crítica
Tipo	Vulnerabilidad de seguridad con explotación activa
Producto afectado	Ecosistema Microsoft Windows
Estado	EXPLOTADO ACTIVAMENTE
Impacto principal	Compromiso de sistemas y servicios afectados



Esta vulnerabilidad representa un riesgo elevado debido a su capacidad potencial para afectar componentes esenciales del ecosistema Microsoft utilizados en ambientes empresariales.

La explotación podría permitir a actores maliciosos comprometer controles de seguridad, ejecutar acciones no autorizadas o afectar servicios tecnológicos utilizados por las organizaciones.

Para el sector salud, la relevancia de esta vulnerabilidad radica en la posibilidad de afectar infraestructura que soporta procesos críticos como autenticación institucional, acceso a aplicaciones internas, servidores administrativos y servicios tecnológicos utilizados durante la operación diaria.

La presencia de explotación activa confirma que los atacantes están utilizando técnicas asociadas a esta vulnerabilidad, por lo cual se recomienda priorizar la aplicación del parche correspondiente y realizar validaciones posteriores para descartar indicadores de compromiso.

Vulnerabilidades Críticas Adicionales de Alta Relevancia

Además de las vulnerabilidades clasificadas como día cero, el ciclo de actualización Microsoft Patch Tuesday de julio de 2026 incluye múltiples fallas críticas y de alta severidad que requieren atención prioritaria debido a su potencial impacto sobre servidores, estaciones de trabajo, servicios de red y aplicaciones empresariales utilizadas por organizaciones del sector salud.

Estas vulnerabilidades afectan componentes fundamentales del ecosistema Microsoft, incluyendo servicios de comunicación de red, autenticación, infraestructura de directorio, herramientas de productividad y plataformas de ejecución utilizadas en ambientes institucionales.



CVE	CVSS	Tipo	Descripción resumida
CVE-2026-33824	9.8	RCE	Windows IKE Extension. Vulnerabilidad crítica de ejecución remota de código sin autenticación mediante el envío de paquetes UDP especialmente diseñados contra servicios IPSec/IKEv2. Un atacante remoto podría comprometer sistemas expuestos que tengan habilitados estos servicios de comunicación segura.
CVE-2026-33827	N/A	RCE	Windows TCP/IP. Vulnerabilidad de ejecución remota de código asociada a una condición de carrera durante el procesamiento de paquetes IPv6 manipulados. Puede afectar sistemas con configuraciones de red específicas y servicios IPSec habilitados.
CVE-2026-33826	8.0	RCE	Windows Active Directory. Vulnerabilidad de ejecución remota de código mediante solicitudes RPC especialmente construidas. Requiere que el atacante tenga acceso a la red adyacente o credenciales dentro del entorno, pudiendo afectar servicios críticos de identidad institucional.
CVE-2026-32157	N/A	RCE	Remote Desktop Client. Vulnerabilidad tipo <i>use-after-free</i> que podría permitir ejecución de código al conectarse a un servidor RDP manipulado por un atacante. Representa riesgo para usuarios que utilizan conexiones remotas hacia entornos no confiables.
CVE-2026-32190	N/A	RCE	Microsoft Office. Vulnerabilidad de ejecución remota de código tipo <i>use-after-free</i> . La explotación requiere que el usuario abra un archivo Office especialmente diseñado, pudiendo comprometer estaciones administrativas o clínicas.



CVE	CVSS	Tipo	Descripción resumida
CVE-2026-33114	N/A	RCE	Microsoft Word. Vulnerabilidad causada por una desreferencia de puntero no confiable. Un atacante podría ejecutar código mediante documentos Word manipulados enviados a usuarios de la organización.
CVE-2026-33115	N/A	RCE	Microsoft Word. Vulnerabilidad adicional tipo <i>use-after-free</i> dentro del procesamiento de documentos. Puede ser utilizada mediante archivos Word maliciosos para comprometer estaciones de trabajo.
CVE-2026-23666	N/A	DoS	.NET Framework. Vulnerabilidad de denegación de servicio asociada a una condición de carrera. Puede ser explotada remotamente mediante solicitudes diseñadas para afectar la disponibilidad de aplicaciones basadas en .NET.

Consecuencias de la Explotación

Estas vulnerabilidades representan un riesgo significativo para instituciones sanitarias debido a la presencia de tecnologías Microsoft en componentes críticos de operación, incluyendo:

- Servidores Windows utilizados para aplicaciones institucionales.
- Controladores de dominio y servicios de autenticación.
- Infraestructura VPN y conexiones IPSec.
- Estaciones de trabajo clínicas y administrativas.
- Plataformas de gestión documental.
- Aplicaciones desarrolladas sobre .NET Framework.
- Herramientas Microsoft Office utilizadas para gestión operativa.



Las vulnerabilidades con mayor prioridad corresponden a aquellas clasificadas como **ejecución remota de código (RCE)**, especialmente las que no requieren autenticación previa, debido a que podrían permitir a un atacante comprometer sistemas directamente desde la red o desde servicios expuestos.

Entre las de mayor criticidad se destacan:

- **CVE-2026-33824 (Windows IKE Extension):** por su puntuación CVSS 9.8 y posibilidad de explotación remota sin autenticación.
- **CVE-2026-33827 (Windows TCP/IP):** por afectar componentes fundamentales de comunicación de red.
- **CVE-2026-33826 (Windows Active Directory):** por el posible impacto sobre servicios de identidad institucional.

Para las organizaciones del sector salud se recomienda priorizar la aplicación de estas actualizaciones en servidores críticos, controladores de dominio, equipos expuestos a internet, infraestructura VPN, estaciones con privilegios elevados y sistemas utilizados para soportar procesos asistenciales y administrativos.

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

Las vulnerabilidades incluidas en el ciclo de actualización Microsoft Patch Tuesday de julio de 2026 presentan diferentes vectores de explotación dependiendo del componente afectado. Los escenarios identificados incluyen explotación remota sin autenticación, elevación de privilegios, abuso de servicios de red, compromiso mediante documentos maliciosos y afectación de servicios críticos de infraestructura.

A continuación, se describen los principales escenarios de explotación:



- **Explotación de CVE-2026-50661 (Windows — Elevación de Privilegios — Explotada Activamente)**

Acceso inicial

El atacante requiere obtener previamente acceso al sistema objetivo mediante credenciales comprometidas, phishing, explotación de otra vulnerabilidad o acceso legítimo de bajo privilegio. Este escenario es frecuente en ataques dirigidos contra organizaciones donde existen estaciones de trabajo con usuarios estándar conectados a dominios corporativos.

Ejecución del componente malicioso

Una vez dentro del sistema, el atacante ejecuta código o herramientas diseñadas para aprovechar la vulnerabilidad presente en los mecanismos internos de Windows relacionados con control de permisos y administración de privilegios.

La falla permite manipular procesos o componentes del sistema operativo para evadir las restricciones establecidas sobre usuarios con privilegios limitados.

Escalamiento de privilegios

Mediante la explotación exitosa, el atacante puede obtener permisos elevados dentro del sistema, potencialmente alcanzando privilegios administrativos o equivalentes al nivel SYSTEM.

Con estos privilegios puede modificar configuraciones de seguridad, acceder a información restringida, deshabilitar controles de protección o preparar ataques adicionales contra otros sistemas de la organización.

Persistencia y movimiento lateral

Con privilegios elevados, el atacante puede establecer mecanismos de persistencia, crear usuarios privilegiados, modificar políticas de seguridad, acceder a recursos compartidos y realizar movimientos laterales hacia servidores, controladores de dominio u otros activos críticos.



En organizaciones del sector salud, este escenario podría comprometer estaciones clínicas, equipos administrativos o servidores conectados a plataformas institucionales.

• **Explotación de CVE-2026-56155 (Windows — Ejecución Remota de Código — Explotada Activamente)**

Identificación del objetivo

El atacante realiza reconocimiento sobre sistemas Windows vulnerables, identificando versiones afectadas, servicios habilitados y posibles puntos de entrada accesibles desde la red interna o externa.

Las actividades pueden incluir análisis de servicios publicados, escaneo de puertos, identificación de versiones del sistema operativo y búsqueda de equipos con componentes vulnerables.

Construcción del mecanismo de explotación

El atacante desarrolla o utiliza una técnica que genera solicitudes especialmente diseñadas para interactuar con el componente vulnerable de Windows.

Estas solicitudes buscan provocar una condición no esperada en el procesamiento del sistema, permitiendo ejecutar instrucciones controladas por el atacante.

Ejecución remota de código

Una explotación exitosa puede permitir que el atacante ejecute código arbitrario en el sistema afectado con los privilegios disponibles para el componente comprometido.

Entre las acciones posteriores pueden incluirse:

- Instalación de malware.
- Descarga de herramientas adicionales.
- Modificación de configuraciones.
- Extracción de información.



- Preparación para movimiento lateral.

Compromiso de infraestructura

En ambientes empresariales, un sistema Windows comprometido puede convertirse en un punto de entrada hacia servicios internos como servidores de aplicaciones, bases de datos, sistemas administrativos o plataformas clínicas.

• Explotación de CVE-2026-56164 (Windows — Vulnerabilidad Crítica con Explotación Activa)

Reconocimiento del entorno

El atacante identifica sistemas Microsoft vulnerables dentro de la organización mediante reconocimiento de red, análisis de servicios y recopilación de información sobre la infraestructura tecnológica.

Explotación del componente vulnerable

El atacante envía solicitudes o ejecuta acciones diseñadas para aprovechar la debilidad identificada en el componente afectado, buscando evadir controles de seguridad o ejecutar acciones no autorizadas.

Obtención de control sobre el sistema

Una explotación exitosa podría permitir afectar la integridad del sistema, ejecutar comandos no autorizados o acceder a recursos protegidos.

El atacante podría utilizar esta condición para:

- Manipular configuraciones.
- Acceder a información sensible.
- Desactivar controles de seguridad.
- Instalar herramientas de persistencia.

Acciones posteriores



Después del compromiso inicial, el atacante puede realizar reconocimiento interno, escalar privilegios, comprometer cuentas adicionales o acceder a sistemas conectados dentro de la organización.

• **Explotación de CVE-2026-33824 (Windows IKE Extension — RCE sin Autenticación — CVSS 9.8)**

Identificación de servicios expuestos

El atacante identifica sistemas Windows que tengan habilitados servicios relacionados con IKEv2/IPSec, comúnmente utilizados en servidores VPN, gateways de acceso remoto y dispositivos que permiten conexiones seguras hacia redes institucionales.

El reconocimiento puede incluir análisis de puertos UDP utilizados por IKE:

- UDP 500.
- UDP 4500.

Construcción del paquete malicioso

El atacante genera paquetes de red especialmente diseñados para interactuar con el servicio vulnerable de Windows IKE.

Estos paquetes buscan provocar errores en el procesamiento interno del servicio, generando condiciones que permitan alterar el flujo normal de ejecución.

Ejecución remota de código

Debido a que la vulnerabilidad no requiere autenticación previa, un atacante remoto podría enviar tráfico malicioso directamente al servicio expuesto y ejecutar código dentro del contexto del proceso vulnerable.

Las acciones posteriores pueden incluir:

- Instalación de cargas maliciosas.
- Creación de accesos persistentes.



- Compromiso del servidor VPN.
- Movimiento lateral hacia redes internas.

Mitigación temporal

Mientras se aplican los parches correspondientes, Microsoft recomienda reducir la exposición del servicio mediante controles de red, incluyendo restricciones sobre tráfico entrante UDP 500 y UDP 4500 desde fuentes no confiables.

• Explotación de CVE-2026-33826 (Windows Active Directory — RCE)

Reconocimiento del dominio

El atacante identifica controladores de dominio, servicios Active Directory y componentes RPC disponibles dentro de la infraestructura.

Envío de solicitudes RPC manipuladas

El atacante genera solicitudes especialmente diseñadas dirigidas a servicios de Active Directory con el objetivo de aprovechar la vulnerabilidad existente en el procesamiento de llamadas remotas.

Ejecución de código

Si la explotación es exitosa, el atacante puede ejecutar código dentro del contexto del servicio comprometido, afectando uno de los componentes más críticos de una organización: la gestión de identidades.

Impacto posterior

El compromiso de Active Directory puede permitir:

- Creación de usuarios privilegiados.
- Alteración de políticas de dominio.
- Acceso a servidores institucionales.



- Compromiso de múltiples sistemas conectados.

En el sector salud, una afectación de Active Directory podría impactar el acceso de usuarios a plataformas clínicas y administrativas.

• **Explotación de CVE-2026-33114 / CVE-2026-33115 (Microsoft Word — RCE mediante documento malicioso)**

Preparación del documento malicioso

El atacante crea documentos de Microsoft Word especialmente diseñados para explotar fallas en el procesamiento interno de archivos.

Los documentos pueden contener estructuras manipuladas que provocan errores de memoria al ser abiertos por versiones vulnerables de Microsoft Word.

Entrega del archivo

El documento malicioso puede distribuirse mediante:

- Correos electrónicos de phishing.
- Sistemas de mensajería corporativa.
- Plataformas de intercambio documental.
- Sitios web comprometidos.

En ataques dirigidos contra el sector salud, los documentos pueden utilizar temáticas relacionadas con:

- Circulares institucionales.
- Informes médicos.
- Documentos administrativos.
- Comunicaciones regulatorias.

Ejecución del código malicioso



Cuando el usuario abre el documento vulnerable, el proceso de Microsoft Word puede ejecutar código controlado por el atacante.

Esto puede permitir:

- Descarga de malware adicional.
- Robo de credenciales.
- Acceso a información local.
- Instalación de herramientas de control remoto.

Persistencia y propagación

Después del compromiso inicial, el atacante puede utilizar la estación afectada para acceder a recursos internos, recolectar información y buscar nuevos objetivos dentro de la red institucional.

Recursos y versiones afectadas:

Las vulnerabilidades corregidas durante el ciclo de actualización **Microsoft Patch Tuesday de julio de 2026** afectan múltiples productos y componentes del ecosistema Microsoft utilizados ampliamente en organizaciones del sector salud. Las entidades deben validar sus inventarios tecnológicos para identificar sistemas operativos, servidores, aplicaciones y servicios que se encuentren en versiones vulnerables o sin las actualizaciones de seguridad correspondientes.

Sistemas Operativos Windows

Sistema Operativo	Versiones / Builds Afectadas
Windows 11	Versiones 23H2, 24H2 y versiones posteriores soportadas con compilaciones anteriores a las actualizaciones acumulativas de julio de 2026
Windows 10	Versión 22H2 con actualizaciones acumulativas de seguridad pendientes del ciclo julio 2026.



Sistema Operativo	Versiones / Builds Afectadas
Windows Server 2025	Instalaciones RTM y versiones con actualizaciones acumulativas anteriores al parche de seguridad de julio de 2026.
Windows Server 2022	Versiones sin las actualizaciones acumulativas de seguridad publicadas en julio de 2026.
Windows Server 2019	Versiones sin actualización acumulativa correspondiente al ciclo julio de 2026.
Windows Server 2016	Versiones sin actualización acumulativa correspondiente al ciclo julio de 2026.

- **Aplicaciones y Servicios Microsoft**

Producto / Componente	Versiones Afectadas
Microsoft SharePoint Server	SharePoint Server Subscription Edition, SharePoint Server 2019 y SharePoint Server 2016 sin actualizaciones acumulativas de seguridad aplicadas.
Microsoft Defender (Antivirus)	Versiones del motor antivirus y plataformas de inteligencia de seguridad anteriores a las actualizaciones publicadas en julio de 2026.
Microsoft Office (Word, Excel)	Office 2016, Office 2019, Office LTSC 2021, Office LTSC 2024 y Microsoft 365 Apps para empresas con versiones vulnerables.
Remote Desktop Client (mstsc.exe)	Clientes RDP integrados en Windows 10, Windows 11 y Windows Server sin actualización de seguridad aplicada.
Windows Active Directory	Servicios de dominio Active Directory ejecutados sobre Windows Server 2016, 2019, 2022 y 2025 sin parches de seguridad actualizados.
Windows IKE Extension	Servicios IKEv2/IPSec habilitados en Windows 10, Windows 11 y versiones Windows Server vulnerables.
Windows TCP/IP Stack	Componentes de red Windows con soporte IPv6 habilitado y sin actualización acumulativa de julio de 2026.



Producto / Componente	Versiones Afectadas
NET Framework	Versiones soportadas de .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 y 4.8.1 sin actualizaciones de seguridad aplicadas.
Windows BitLocker	Sistemas Windows con BitLocker habilitado y componentes relacionados sin actualización del ciclo julio 2026.
Windows Hello	Componentes de autenticación biométrica en Windows 10 y Windows 11 sin actualización de seguridad.
Windows Kerberos	Sistemas unidos a dominio Active Directory con componentes Kerberos vulnerables sin parche aplicado.
Azure Monitor Agent / Logic Apps	Versiones anteriores a las actualizaciones de seguridad publicadas por Microsoft en julio de 2026.
SQL Server	SQL Server 2019, SQL Server 2022 y ediciones compatibles sin actualizaciones acumulativas de seguridad aplicadas.
Microsoft Edge (Chromium)	Versiones anteriores a las actualizaciones de seguridad acumulativas del navegador correspondientes al ciclo de julio de 2026.

Vector de impacto:



Las vulnerabilidades corregidas durante el ciclo de actualización Microsoft Patch Tuesday de julio de 2026 presentan diferentes vectores de impacto que pueden afectar la confidencialidad, integridad y disponibilidad de los activos tecnológicos utilizados por las organizaciones del sector salud.

La distribución de vulnerabilidades evidencia una mayor concentración en fallas de elevación de privilegios (EoP), ejecución remota de código (RCE) y divulgación de información, categorías que representan un riesgo elevado debido a su capacidad para comprometer sistemas operativos, servidores institucionales, servicios de autenticación y estaciones de trabajo utilizadas en procesos clínicos y administrativos.



• Elevación de Privilegios (EoP)

Este fue el vector de impacto con mayor presencia dentro del ciclo de actualización, con aproximadamente 254 vulnerabilidades identificadas.

Las vulnerabilidades de elevación de privilegios permiten que un atacante con acceso inicial limitado a un sistema pueda obtener permisos superiores, llegando potencialmente a privilegios administrativos o nivel SYSTEM.

En ambientes del sector salud, este tipo de vulnerabilidad representa un riesgo crítico debido a que un atacante podría utilizar un equipo comprometido como punto inicial para ampliar su acceso hacia servidores institucionales, controladores de dominio, aplicaciones clínicas o sistemas administrativos.

Las fallas EoP suelen ser utilizadas como una segunda fase dentro de ataques más complejos, permitiendo evadir restricciones, modificar configuraciones de seguridad, acceder a información protegida y facilitar movimientos laterales dentro de la red corporativa.

• Ejecución Remota de Código (RCE)

Durante este ciclo se corrigieron aproximadamente 145 vulnerabilidades asociadas a ejecución remota de código (RCE).

Las vulnerabilidades RCE representan uno de los mayores riesgos dentro de la gestión de seguridad debido a que pueden permitir que un atacante ejecute instrucciones arbitrarias en un sistema afectado sin requerir acceso físico.

Dependiendo del componente vulnerable, un atacante podría comprometer servidores, estaciones de trabajo, servicios de red o aplicaciones empresariales mediante solicitudes especialmente diseñadas, archivos maliciosos o explotación de servicios expuestos.

Para organizaciones del sector salud, estas vulnerabilidades pueden afectar directamente la continuidad operacional al comprometer sistemas utilizados para:

- Gestión de usuarios.



- Aplicaciones administrativas.
- Plataformas clínicas.
- Servicios de acceso remoto.
- Servidores de infraestructura.

• Divulgación de Información

Se corrigieron aproximadamente 102 vulnerabilidades relacionadas con divulgación de información.

Estas fallas pueden permitir que un atacante acceda a información que debería permanecer protegida, incluyendo datos almacenados en memoria, archivos internos, configuraciones del sistema, credenciales, metadatos o información utilizada por aplicaciones institucionales.

En el sector salud, este tipo de vulnerabilidad representa un riesgo relevante debido al tratamiento de información sensible asociada a:

- Datos personales de pacientes.
- Información clínica.
- Información administrativa.
- Credenciales de usuarios.
- Configuraciones internas de infraestructura tecnológica.

• Denegación de Servicio (DoS)

Durante el ciclo de actualización se corrigieron aproximadamente 35 vulnerabilidades de denegación de servicio (DoS).



Estas vulnerabilidades pueden permitir que un atacante provoque la interrupción parcial o total de un servicio mediante solicitudes diseñadas para consumir recursos del sistema, generar errores o provocar fallos en componentes específicos.

La explotación de estas fallas puede afectar la disponibilidad de servicios tecnológicos utilizados en instituciones de salud, incluyendo:

- Servidores institucionales.
- Servicios de autenticación.
- Aplicaciones administrativas.
- Plataformas de comunicación.
- Sistemas integrados con procesos asistenciales.

● **Omisión de funciones de seguridad (Security Feature Bypass)**

Se corrigieron aproximadamente 17 vulnerabilidades relacionadas con la omisión de funciones de seguridad.

Estas vulnerabilidades permiten que un atacante evada mecanismos de protección diseñados para restringir acciones no autorizadas dentro del sistema.

Una explotación exitosa podría permitir:

- Evadir controles de autenticación.
- Saltar restricciones de seguridad.
- Ejecutar acciones normalmente bloqueadas.
- Reducir la efectividad de mecanismos de protección existentes.

En entornos hospitalarios, estas fallas pueden aumentar el impacto de otros ataques al permitir superar controles implementados sobre sistemas críticos.



• Suplantación de Identidad (Spoofing)

Se corrigieron aproximadamente 16 vulnerabilidades de spoofing.

Estas fallas permiten que un atacante pueda hacerse pasar por otro usuario, servicio o componente confiable con el objetivo de engañar mecanismos de validación o usuarios legítimos.

Los riesgos asociados incluyen:

- Acceso mediante identidades falsas.
- Manipulación de comunicaciones.
- Robo de confianza entre sistemas.
- Obtención de información protegida.

Para entidades de salud, estas vulnerabilidades pueden afectar mecanismos de autenticación, comunicaciones internas y servicios integrados con proveedores externos.

• Manipulación (Tampering)

Las vulnerabilidades relacionadas con manipulación afectan la integridad de los sistemas y la información procesada.

Un atacante podría intentar modificar:

- Archivos del sistema.
- Configuraciones de aplicaciones.
- Registros de actividad (*logs*).
- Información almacenada.
- Datos transmitidos entre sistemas.



Aunque este vector tiene menor representación dentro del ciclo de julio de 2026, su impacto puede ser significativo en organizaciones sanitarias, donde la integridad de la información clínica y administrativa es fundamental para garantizar procesos confiables y trazables.

Recomendaciones de mitigación:

Las siguientes acciones deben ejecutarse de forma transversal sobre todos los sistemas, servidores, estaciones de trabajo y servicios Microsoft afectados identificados dentro del ciclo de actualización Patch Tuesday de julio de 2026:

1. Aplicar las actualizaciones de seguridad de julio de 2026 de Microsoft:

Implementar los parches acumulativos mediante los mecanismos corporativos disponibles como Windows Update, Windows Server Update Services (WSUS), Microsoft Configuration Manager (SCCM) o Microsoft Intune, garantizando cobertura sobre servidores, estaciones clínicas, equipos administrativos y ambientes de contingencia.

2. Priorizar la actualización de vulnerabilidades con explotación activa:

Dar tratamiento prioritario a las vulnerabilidades clasificadas como día cero o explotadas activamente, especialmente:

- **CVE-2026-50661:** Vulnerabilidad de elevación de privilegios en Windows.
- **CVE-2026-56155:** Vulnerabilidad de ejecución remota de código en componentes Microsoft.
- **CVE-2026-56164:** Vulnerabilidad crítica con explotación activa.

La aplicación de estos parches debe priorizarse en servidores críticos, equipos con privilegios administrativos y activos expuestos a internet.



3. Actualizar componentes de infraestructura crítica:

Priorizar la instalación de actualizaciones en:

- Controladores de dominio Active Directory.
- Servidores Windows institucionales.
- Servicios VPN/IPSec.
- Servidores SharePoint.
- Servidores de aplicaciones.
- Equipos utilizados para acceso remoto.

4. Mitigar temporalmente exposición de Windows IKE/IPSec (CVE-2026-33824):

En los casos donde no sea posible aplicar inmediatamente el parche correspondiente, implementar controles temporales de red:

- Restringir tráfico entrante UDP 500.
- Restringir tráfico entrante UDP 4500.
- Permitir únicamente conexiones desde redes autorizadas.
- Revisar exposición de servicios VPN hacia internet.

5. Fortalecer Microsoft Defender y soluciones EDR/XDR:

Verificar que todos los equipos cuenten con:

- Motor antivirus actualizado.
- Inteligencia de seguridad vigente.



- Protección en tiempo real habilitada.
- Monitoreo de comportamiento activo.

Esto permite reducir el riesgo asociado a explotación posterior de vulnerabilidades de elevación de privilegios y ejecución de código.

6. Aplicar actualizaciones de Microsoft Office:

Actualizar todas las estaciones de trabajo utilizadas para procesamiento de documentos Office, especialmente aquellas donde se manejan:

- Documentación clínica.
- Informes administrativos.
- Comunicaciones institucionales.
- Archivos compartidos con terceros.

Esto reduce el riesgo asociado a vulnerabilidades de ejecución remota de código mediante documentos manipulados.

7. Revisar configuraciones IPv6 y componentes de red:

Para reducir la superficie de ataque asociada a vulnerabilidades en componentes TCP/IP:

- Validar el uso real de IPv6 dentro de la organización.
- Deshabilitar IPv6 únicamente en segmentos donde no sea requerido.
- Aplicar reglas de filtrado de tráfico para servicios no utilizados.



Mitigaciones adicionales y Hardening

- **Implementar el principio de mínimo privilegio:**

Garantizar que usuarios clínicos, administrativos y operativos trabajen con cuentas estándar, evitando privilegios de administrador local innecesarios. Esto limita el impacto de vulnerabilidades de elevación de privilegios.

- **Fortalecer Active Directory:**

Aplicar medidas de endurecimiento sobre servicios de identidad:

- Revisar grupos privilegiados.
- Implementar controles sobre cuentas administrativas.
- Activar mecanismos de protección contra robo de credenciales.
- Reducir riesgos asociados a técnicas como Pass-the-Hash y Pass-the-Ticket.

- **Implementar autenticación multifactor (MFA):**

Aplicar MFA en accesos críticos, especialmente:

- Administradores de sistemas.
- Accesos remotos.
- Servicios publicados hacia internet.
- Plataformas administrativas.

- **Fortalecer protección de correo electrónico:**

Configurar filtros avanzados para:



- Bloquear archivos Office sospechosos.
- Analizar documentos adjuntos.
- Aplicar cuarentena a archivos provenientes de remitentes no confiables.
- Detectar campañas de phishing dirigidas.

- **Habilitar mecanismos de protección en Microsoft Office:**

Implementar mediante políticas corporativas:

- Protected View.
- Microsoft Defender Application Guard cuando aplique.
- Bloqueo de macros VBA provenientes de internet.
- Restricciones para ejecución de contenido activo.

- **Implementar segmentación de red y controles NAC:**

Aplicar controles de acceso de red para limitar comunicaciones entre segmentos críticos, especialmente:

- Controladores de dominio.
- Servidores clínicos.
- Bases de datos.
- Servidores administrativos.



Esto reduce la posibilidad de movimiento lateral posterior a un compromiso.

- **Fortalecer servicios de acceso remoto:**

Revisar configuraciones de:

- Remote Desktop Services.
- VPN institucionales.
- Servicios publicados externamente.

Aplicar restricciones de acceso, monitoreo de sesiones y autenticación reforzada.

- **Verificar actualizaciones automáticas en endpoints:**

Confirmar que todas las estaciones del parque tecnológico tengan habilitado:

- Actualización automática de Windows.
- Actualización de Microsoft Defender.
- Instalación periódica de parches críticos.

- **Monitorear indicadores de compromiso:**

Revisar eventos asociados a:

- Elevación inesperada de privilegios.
- Creación de usuarios administrativos.
- Ejecución de procesos desconocidos.
- Accesos anómalos a servidores.



- Cambios no autorizados en configuraciones.

Fuentes:



Microsoft Security Response Center (MSRC) — Security Update Guide, Patch Tuesday julio 2026

Guía oficial de Microsoft con el detalle de vulnerabilidades corregidas, productos afectados, severidad, puntuaciones CVSS, actualizaciones disponibles y recomendaciones de seguridad.
o URL: <https://msrc.microsoft.com/update-guide>

CISA Known Exploited Vulnerabilities Catalog (KEV)

Catálogo oficial de vulnerabilidades explotadas activamente utilizado para priorización de remediación. Incluye vulnerabilidades Microsoft con evidencia de explotación en escenarios reales.

o URL: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

National Vulnerability Database (NVD) — National Institute of Standards and Technology (NIST)

Base de datos técnica con información detallada de vulnerabilidades CVE, clasificación CVSS, vectores de ataque y referencias asociadas.
o URL: <https://nvd.nist.gov/>

Microsoft Security Update Guide — CVE-2026-50661, CVE-2026-56155 y CVE-2026-56164

Información oficial de Microsoft sobre vulnerabilidades de día cero, productos afectados y actualizaciones de seguridad correspondientes al ciclo julio 2026.
o URL: <https://msrc.microsoft.com/update-guide>

Qualys — Microsoft Patch Tuesday July 2026 Security Update Review
Análisis técnico independiente sobre las vulnerabilidades corregidas por Microsoft, impacto,



priorización y recomendaciones de parcheo empresarial.
o URL: <https://blog.qualys.com/>

Tenable — Microsoft Patch Tuesday July 2026 Security Updates
Análisis de vulnerabilidades Microsoft, evaluación de riesgo y recomendaciones para gestión de exposición tecnológica.
o URL: <https://www.tenable.com/blog>

Cisco Talos Intelligence — Microsoft Patch Tuesday July 2026: Snort Rules and Prominent Vulnerabilities
Análisis técnico de vulnerabilidades relevantes, indicadores de detección y reglas de monitoreo asociadas mediante Snort.
o URL: <https://blog.talosintelligence.com/>

Lansweeper — Microsoft Patch Tuesday July 2026
Análisis de activos afectados, identificación de versiones vulnerables y recomendaciones para administración de parches en entornos empresariales.
o URL: <https://www.lansweeper.com/blog/>

BleepingComputer — Microsoft July 2026 Patch Tuesday Security Updates
Resumen técnico de vulnerabilidades corregidas, fallas críticas y vulnerabilidades de día cero abordadas durante el ciclo de actualización.
o URL: <https://www.bleepingcomputer.com/>

MITRE ATT&CK Framework
Marco de referencia utilizado para contextualizar técnicas de ataque asociadas a explotación de vulnerabilidades, escalamiento de privilegios, ejecución remota de código y movimiento lateral.
o URL: <https://attack.mitre.org>



**Windows Release Health / Microsoft Update Catalog — Actualizaciones acumulativas
Windows julio 2026**

Repositorio oficial de Microsoft para consultar paquetes acumulativos, números KB, versiones corregidas y requisitos de instalación para sistemas Windows.
o URL: <https://catalog.update.microsoft.com/>

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.

