Boletín informativo

CSIRTSALUD-AL-20260415-91

TLP: CLEAR

Alerta ID:	091
Fecha del reporte:	15/04/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades en Patch Tuesday de Microsoft – Abril 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 marzo de 2026, abordando un total de **165 vulnerabilidades** en múltiples productos y componentes del ecosistema Windows y servicios en la nube. Este documento busca priorizar la mitigación de vulnerabilidades críticas y de día cero para garantizar la continuidad operativa de los servicios de salud y proteger la infraestructura tecnológica contra vectores de ataque emergentes, enfocándose en resultados a nivel de servicio y resiliencia de la red.

Concientizando sobre los riesgos de explotación, facilitando la identificación de activos y versiones afectadas, promoviendo la aplicación oportuna de parches y medidas de mitigación, y fortaleciendo la capacidad de respuesta ante incidentes de seguridad.

Boletín informativo

CSIRTSALUD-AL-20260415-91

TLP: CLEAR

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 Windows, Microsoft Office, SharePoint, Active Directory, .NET, Azure y herramientas de desarrollo.

El ciclo de Patch Tuesday de abril de 2026, publicado el 14 de abril de 2026, es uno de los más voluminosos en la historia reciente del programa. A continuación se presenta el resumen estadístico:

Categoría	Cantidad
Total de vulnerabilidades corregidas	165 CVEs
Vulnerabilidades Críticas	8
Vulnerabilidades Importantes	155
Moderadas / Bajas	1 moderada + 1 baja
Día cero explotado activamente	1 (CVE-2026-32201)
Día cero divulgado públicamente	1 (CVE-2026-33825)
RCE Críticas	7
DoS Críticas	1

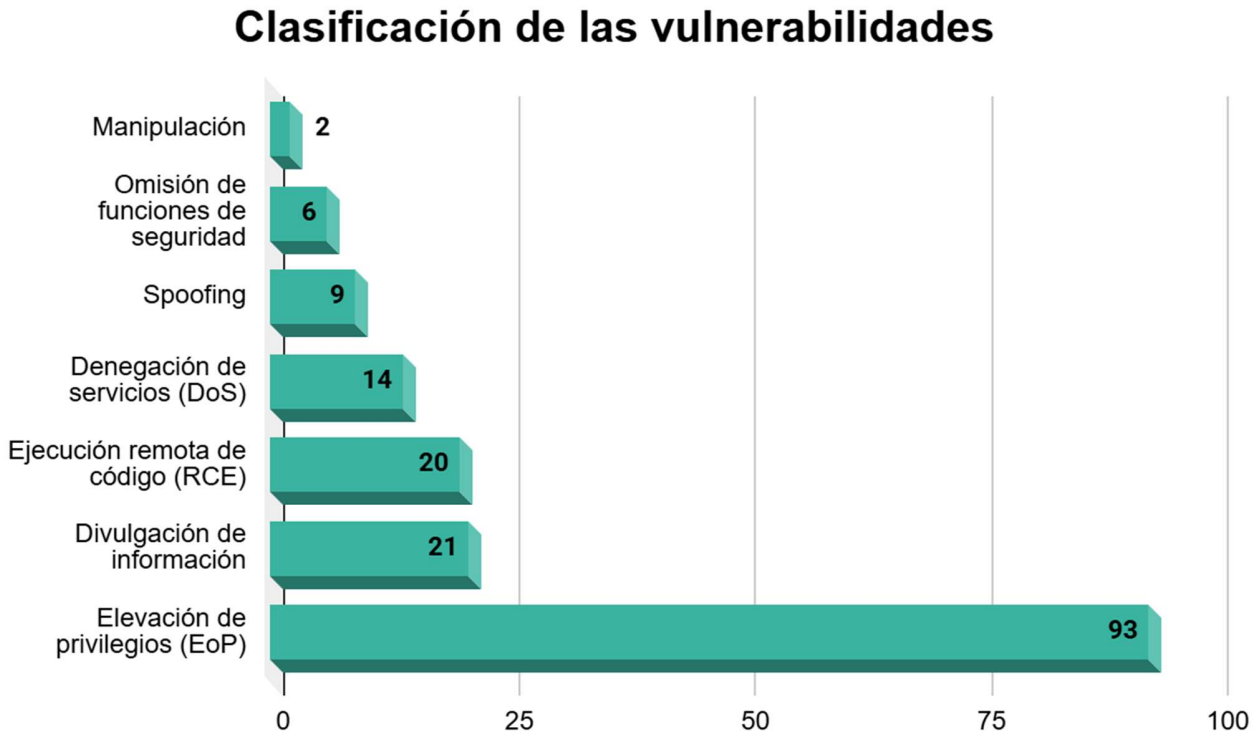
Las familias de productos afectados incluyen: Windows Boot Loader, Windows Kernel, Windows Active Directory, Windows IKE Extension, Windows TCP/IP, Microsoft Office (Word,

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:

Manipulación: 2
Omisión de funciones de seguridad: 6
Spoofing: 9
Denegación de servicios (DoS): 14
Ejecución remota de código (RCE): 20
Divulgación de información: 21
Elevación de privilegios (EoP): 93



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-2026-33825
CVSS v3	7.8 (Importante)
Tipo	Elevation of Privilege (EoP) — Control de acceso insuficiente
Producto afectado	Microsoft Defender (Windows)
Estado	DIVULGADO PÚBLICAMENTE — Exploit en GitHub (alias: BlueHammer)
Exploit público	Publicado el 3 de abril de 2026 por 'Chaotic Eclipse'

Esta falla en Microsoft Defender presenta una granularidad de control de acceso insuficiente (Insufficient Granularity of Access Control), lo que permite a un atacante autenticado con privilegios bajos elevar sus permisos hasta nivel SYSTEM. El exploit BlueHammer fue publicado en GitHub el 3 de abril de 2026 por un investigador con el alias 'Chaotic Eclipse', quien expresó malestar por el proceso de divulgación responsable con Microsoft antes de que el parche estuviera disponible.

Al ser un exploit funcional de dominio público, el riesgo de explotación masiva es elevado. Cualquier actor de amenaza con acceso inicial al sistema podría aprovecharlo para escalar privilegios y comprometer el entorno completo.

Vulnerabilidades Críticas Adicionales de Alta Relevancia.

CVE	CVSS	Tipo	Descripción resumida
CVE-2026-33824	9.8	RCE	Windows IKE Extension — RCE sin autenticación mediante paquetes UDP maliciosos (IPSec/IKEv2). El más crítico del ciclo.
CVE-2026-33827	N/A	RCE	Windows TCP/IP — RCE por condición de carrera mediante paquetes IPv6 maliciosos contra nodos con IPSec habilitado.
CVE-2026-33826	8.0	RCE	Windows Active Directory — RCE mediante llamadas RPC especialmente construidas por un atacante autenticado en red adyacente.
CVE-2026-32157	N/A	RCE	Remote Desktop Client — RCE tipo use-after-free. El usuario debe conectarse a un servidor RDP malicioso.
CVE-2026-32190	N/A	RCE	Microsoft Office — RCE tipo use-after-free. Explotación local tras abrir un archivo Office malicioso.
CVE-2026-33114	N/A	RCE	Microsoft Word — RCE por derreferencia de puntero no confiable. Ejecución local al abrir documento Word manipulado.
CVE-2026-33115	N/A	RCE	Microsoft Word — RCE tipo use-after-free. Complementaría a CVE-2026-33114; misma superficie de ataque en Word.
CVE-2026-23666	N/A	DoS	.NET Framework — Denegación de servicio por condición de carrera. No requiere autenticación; ataque por red.

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:

Compromiso de Confidencialidad e Integridad (CVE-2026-32201 — SharePoint)

- Acceso no autorizado a documentos clínicos, contratos, datos de pacientes y comunicaciones internas almacenadas en SharePoint.
- Modificación de información divulgada, lo que podría alterar registros médicos o documentos regulatorios.
- Uso del servidor SharePoint comprometido como punto de pivote para ataques de phishing internos (suplantación de identidad organizacional).

Escalada de Privilegios hasta SYSTEM (CVE-2026-33825 — Defender BlueHammer)

- Un atacante con acceso inicial limitado puede obtener control total del sistema operativo.
- Desactivación de controles de seguridad, incluyendo el propio Microsoft Defender y soluciones EDR.
- Instalación de malware persistente, backdoors, ransomware o herramientas de acceso remoto (RAT).
- Exfiltración masiva de datos de salud (PHI/ePHI) y datos corporativos sensibles.

Ejecución Remota de Código sin Autenticación (CVE-2026-33824, CVE-2026-33827)

- Compromiso total de sistemas expuestos a internet con IKEv2 o IPSec habilitado.
- Movimiento lateral en redes hospitalarias hacia sistemas PACS, HIS/RIS, EMR y servidores de bases de datos.
- Posible despliegue de ransomware dirigido a infraestructura crítica de salud.
- Interrupción de servicios clínicos esenciales (atención de urgencias, laboratorios, imagenología).

Compromiso de Active Directory (CVE-2026-33826)

- Ejecución de código en el host RPC con los permisos del servicio comprometido.
- Posible toma de control de controladores de dominio (Domain Controller takeover).
- Persistencia avanzada mediante creación de cuentas privilegiadas o modificación de GPOs.

- Acceso a todos los sistemas autenticados por el dominio, incluyendo aplicaciones clínicas.

Explotación a través de Documentos Office (CVE-2026-32190, CVE-2026-33114, CVE-2026-33115)

- Ejecución de código malicioso al abrir un archivo Word, Excel o documento Office manipulado.
- Vector ideal para campañas de spear-phishing dirigidas a personal médico y administrativo.
- Descarga y ejecución de cargas maliciosas (stealers, loaders, ransomware) en el endpoint del usuario.

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

- **Explotación de CVE-2026-32201 (SharePoint — Spoofing — Activamente Explotado)**

Reconocimiento: El atacante identifica instancias de Microsoft SharePoint Server accesibles en la red, ya sea mediante herramientas de escaneo pasivo (Shodan, Censys) o reconocimiento activo (nmap, whatweb). Verifica la versión del servidor mediante cabeceras HTTP (X-SharePointHealthScore, MicrosoftSharePointTeamServices) o respuestas de páginas de error.

Construcción del payload: El atacante elabora una solicitud HTTP/HTTPS especialmente diseñada que omite los controles de validación de entrada del servidor SharePoint. La solicitud no incluye un token de autenticación válido pero está estructurada para evadir las verificaciones del endpoint mediante la manipulación de parámetros de la API REST de SharePoint (/_api/web/, /_vti_bin/).

Explotación: Al enviar la solicitud maliciosa al servidor, el motor de validación de SharePoint procesa incorrectamente el input, permitiendo al atacante no autenticado realizar operaciones privilegiadas: lectura de metadatos sensibles, modificación de permisos de sitios, suplantación de identidad de usuarios mediante tokens de sesión manipulados, y en algunos escenarios, enumeración de usuarios y grupos del dominio.

Post-explotación: Con los datos obtenidos (tokens, credenciales en documentos, información de la estructura organizacional), el atacante puede lanzar ataques de spear-phishing internos, acceder a sistemas adicionales o exfiltrar documentos clínicos y administrativos de alto valor.

- **Explotación de CVE-2026-33825 (Defender EoP — BlueHammer)**

Acceso inicial: El atacante obtiene acceso inicial al sistema objetivo con privilegios bajos (usuario estándar) mediante phishing, explotación de otra vulnerabilidad o credenciales comprometidas disponibles en mercados de logs (RedLine, Lumma, Vidar).

Descarga del exploit: El exploit BlueHammer, disponible públicamente en GitHub desde el 3 de abril de 2026, es descargado al sistema víctima. El exploit aprovecha la granularidad insuficiente de control de acceso en Windows Defender (MsMpEng.exe) para manipular objetos de seguridad internos del proceso protegido.

Escalada de privilegios: El exploit abusa de un handle de proceso mal controlado dentro de MsMpEng.exe para inyectar código o modificar tokens de acceso, resultando en la obtención de un token de SYSTEM. Este token permite al atacante ejecutar cualquier proceso con privilegios máximos en el sistema.

Persistencia y movimiento lateral: Con privilegios SYSTEM, el atacante puede deshabilitar controles de seguridad, crear cuentas de administrador, instalar backdoors en el registro o en carpetas del sistema, y proceder al movimiento lateral usando Pass-the-Hash, Pass-the-Ticket o WMI remoto.

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

Identificación de objetivos: El atacante identifica hosts Windows con el servicio IKE versión 2 habilitado (comúnmente en servidores VPN, gateways de red) usando escaneos de puertos UDP 500 y 4500.

Construcción del paquete malicioso: Se construyen paquetes IKEv2 especialmente diseñados que provocan corrupción de memoria en el proceso del servicio IKE de Windows. La vulnerabilidad es de tipo double free, donde la misma región de memoria es liberada dos veces, permitiendo al atacante controlar el flujo de ejecución del proceso.

Ejecución de código: El atacante envía los paquetes UDP maliciosos al host objetivo. Sin requerir ninguna autenticación previa, el proceso del servicio IKE ejecuta el shellcode del atacante con los privilegios del servicio de red. Esto puede resultar en la instalación inmediata de un backdoor, descarga de cargas maliciosas adicionales o inicio de movimiento lateral.

Mitigación temporal disponible: Microsoft recomienda como medida de mitigación temporal (si el parche no puede aplicarse inmediatamente) implementar reglas de firewall para bloquear el tráfico entrante en UDP 500 y UDP 4500 desde fuentes no confiables.

- **Explotación de CVE-2026-33114 / CVE-2026-33115 (Microsoft Word — RCE por Documento Malicioso)**

Preparación del documento: El atacante crea un archivo .docx o .rtf especialmente diseñado que contiene un puntero no confiable (CVE-2026-33114) o una estructura de objeto que libera memoria dos veces (CVE-2026-33115 — use-after-free) al ser procesado por el motor de Word.

Entrega: El documento malicioso es distribuido mediante correo electrónico de phishing, adjuntos en sistemas de mensajería o descarga desde sitios web comprometidos. El asunto del correo suele ser relevante para el sector objetivo (p. ej., 'Circular ADRES 2026', 'Resolución Minsalud', 'Informe laboratorio', 'Resultado examen médico').

Ejecución: Cuando el usuario abre el documento con una versión vulnerable de Microsoft Word, el proceso WINWORD.EXE accede a una región de memoria inválida. El atacante controla esta región mediante técnicas de heap spraying o grooming, logrando redirigir la ejecución hacia su shellcode, que generalmente descarga y ejecuta una carga maliciosa de primera etapa (dropper/loader).

Recursos y versiones afectadas:

- **Sistemas Operativos Windows**

Sistema Operativo	Versiones / Builds Afectadas
Windows 11	Versiones 23H2, 24H2, 25H2 (Build 26200.x) — KB5083769
Windows 10	Versión 22H2 — KB5082200 (Extended Security Update)
Windows Server 2025	Todas las versiones RTM y cumulative updates anteriores a abril 2026
Windows Server 2022	Todas las versiones anteriores al parche de abril 2026

Sistema Operativo	Versiones / Builds Afectadas
Windows Server 2019	Todas las versiones anteriores al parche de abril 2026
Windows Server 2016	Todas las versiones anteriores al parche de abril 2026

- **Aplicaciones y Servicios Microsoft**

Producto / Componente	Versiones Afectadas
Microsoft SharePoint Server	SharePoint Server Subscription Edition, 2019, 2016
Microsoft Defender (Antivirus)	Versiones de definición y motor anteriores a abril 2026
Microsoft Office (Word, Excel)	Office 2016, 2019, 2021, Microsoft 365 Apps para empresas
Remote Desktop Client (mstsc.exe)	Clientes RDP integrados en Windows 10/11 y Server
Windows Active Directory	AD DS en Windows Server 2016/2019/2022/2025
Windows IKE Extension	Servicio IKEv2 en Windows 10/11 y todas las versiones Server
Windows TCP/IP Stack	Stack de red con IPv6 habilitado en Windows 10/11 y Server
NET Framework	.NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8, 4.8.1
Windows BitLocker	BitLocker en Windows 10/11 y Windows Server con Secure Boot
Windows Hello	Componente de autenticación biométrica en Windows 10/11
Windows Kerberos	Kerberos integrado en sistemas unidos a dominio AD
Azure Monitor Agent / Logic Apps	Versiones anteriores a las actualizaciones de abril 2026
SQL Server	SQL Server 2019, 2022 en todas las ediciones
Microsoft Edge (Chromium)	Versiones anteriores a las 80 correcciones del mes (Google)

Vector de impacto:

- **Elevación de Privilegios (EoP)**

Este fue el vector de impacto más predominante, con alrededor de **93 vulnerabilidades**. Una vulnerabilidad de elevación de privilegios permite a un atacante con acceso limitado a un sistema obtener mayores privilegios, como los de un administrador. Esto a menudo se utiliza como un segundo paso después de haber obtenido un acceso inicial, para así tomar control total del sistema afectado.

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

Se corrigieron aproximadamente **20 vulnerabilidades** de este tipo. Las vulnerabilidades de RCE son particularmente críticas porque permiten a un atacante ejecutar código malicioso en un sistema vulnerable a través de una red, sin necesidad de acceso físico. Esto puede llevar al compromiso total del sistema.

- **Divulgación de información**

Se abordaron cerca de **21 vulnerabilidades** de este tipo. Estas fallas de seguridad podrían permitir a un atacante acceder a información sensible que normalmente estaría protegida en un sistema.

- **Denegación de Servicio (DoS)**

También se solucionaron alrededor de 1**4 vulnerabilidades** de DoS. Un ataque de denegación de servicio tiene como objetivo hacer que un sistema o servicio no esté disponible para sus usuarios legítimos, interrumpiendo su funcionamiento.

- **Omisión de funciones de seguridad:**

Se solucionaron alrededor de **6 vulnerabilidades** Estas vulnerabilidades permiten saltarse mecanismos de seguridad diseñados para proteger Windows, sin necesidad de romperlos directamente.

- **Suplantación de Identidad (Spoofing)**

Se corrigieron unas **9 vulnerabilidades** de este tipo, las cuales podrían permitir a un atacante hacerse pasar por otra persona o sistema para ganar la confianza de un usuario y robar información o realizar otras acciones maliciosas.

- **Manipulación**

Se corrigieron **2 vulnerabilidades** de este tipo, el objetivo principal del *tampering* es romper la integridad de un sistema. El atacante busca alterar cómo funciona algo o la información que contiene como Logs, datos en Tránsito, entre otros, generalmente para beneficiarse de ese cambio, evadir controles o causar daño.

Recomendaciones de mitigación:

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

1. Aplicar las actualizaciones de seguridad de abril 2026 de Microsoft vía Windows Update, WSUS o SCCM/Intune para todos los sistemas Windows del inventario.
2. Priorizar el parcheo de SharePoint Server (CVE-2026-32201 — explotado activamente), Microsoft Defender (CVE-2026-33825), Windows IKE (CVE-2026-33824 — CVSS 9.8) y Active Directory (CVE-2026-33826).

3. Si el parcheo inmediato de CVE-2026-33824 no es posible, implementar reglas de firewall para bloquear el tráfico entrante en UDP 500 y UDP 4500 desde fuentes externas no confiables.
4. Actualizar las definiciones de Microsoft Defender a la versión más reciente de inmediato para mitigar el riesgo de explotación de BlueHammer (CVE-2026-33825).
5. Aplicar las actualizaciones de Microsoft Office en todas las estaciones de trabajo de usuarios que manipulen documentos Word o Excel para mitigar CVE-2026-32190, CVE-2026-33114 y CVE-2026-33115.
6. Deshabilitar IPv6 en segmentos de red donde no sea requerido para reducir la superficie de ataque de CVE-2026-33827.

Mitigaciones Adicionales y Hardening

- Implementar el Principio de Mínimo Privilegio: asegurar que los usuarios clínicos y administrativos operen con cuentas de usuario estándar, sin privilegios de administrador local, para limitar el impacto de la explotación de CVE-2026-33825.
- Habilitar Protected Users Security Group en Active Directory para reducir el riesgo de explotación de técnicas de movimiento lateral (Pass-the-Hash, Pass-the-Ticket).
- Configurar el filtrado de adjuntos en las soluciones de correo electrónico para bloquear o poner en cuarentena automáticamente archivos .docx, .docm, .rtf y .xlsx de remitentes externos no verificados.
- Activar Protected View y Application Guard en Microsoft Office para aislar la apertura de documentos provenientes de fuentes externas.
- Habilitar el bloqueo de macros VBA por defecto en Microsoft Office mediante GPO, siguiendo las directrices de endurecimiento de Microsoft.
- Implementar Network Access Control (NAC) o segmentación de red para limitar el acceso de red adyacente al Controlador de Dominio únicamente a hosts autorizados (mitiga CVE-2026-33826).

- Verificar que las actualizaciones automáticas de Windows Defender estén habilitadas en todos los endpoints del parque tecnológico del sector salud.
- Revisar y aplicar el nuevo diálogo de advertencia de RDP introducido en la actualización de abril 2026 para proteger a usuarios de servidores RDP maliciosos.

Fuentes:

- Microsoft Security Response Center (MSRC) — Guía de actualizaciones de abril 2026: https://msrc.microsoft.com/update-guide
- CISA Known Exploited Vulnerabilities Catalog — CVE-2026-32201: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Qualys — Microsoft and Adobe Patch Tuesday, April 2026 Security Update Review
- Tenable — Microsoft's April 2026 Patch Tuesday Addresses 163 CVEs (CVE-2026-32201)
- Cisco Talos Intelligence — Microsoft Patch Tuesday for April 2026: Snort Rules and Prominent Vulnerabilities
- Lansweeper — Microsoft Patch Tuesday April 2026
- BleepingComputer — Microsoft April 2026 Patch Tuesday fixes 167 flaws, 2 zero-days
- MITRE ATT&CK Framework v15 — https://attack.mitre.org
- Windows 11 KB5083769 April 2026 Patch Tuesday Update — Microsoft

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.