Alerta Vulnerabilidad
Vulnerabilidades CVE-2026-32201 y CVE-2026-33825 Microsoft

CSIRTSALUD-AV-20260430-43 **TLP: CLEAR**

Alerta ID:	043
Fecha del reporte:	30/04/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades CVE-2026-32201 y CVE-2026-33825 Microsoft
Herramienta de detección	N/A
Activo involucrado:	Microsoft
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades gubernamentales y a las organizaciones del ecosistema digital sobre las vulnerabilidades críticas identificadas en varios productos de Microsoft, que están siendo explotadas activamente. La CISA ha añadido estas vulnerabilidades a su Catálogo de Vulnerabilidades Explotadas y ha instado a todas las organizaciones a aplicar las actualizaciones de seguridad lo antes posible.

Descripción:

Microsoft ha lanzado actualizaciones de seguridad para corregir vulnerabilidades críticas en productos como Microsoft Defender, .NET y Microsoft SQL Server. Entre estas, las vulnerabilidades **CVE-2026-32201 y CVE-2026-33825** están siendo explotadas activamente por ciberdelincuentes y permiten la escalada de privilegios, lo que podría darles acceso no

autorizado a recursos del sistema. Debido a la gravedad de estos riesgos, la CISA ha incluido estas vulnerabilidades en su Catálogo de Vulnerabilidades Explotadas. Se recomienda aplicar las actualizaciones de seguridad de inmediato para evitar posibles ataques y proteger los sistemas afectados.

Consecuencias de la explotación

La explotación exitosa de las vulnerabilidades identificadas, como **CVE-2026-32201 y CVE-2026-33825**, puede tener un impacto significativo tanto a nivel técnico como operativo en las organizaciones afectadas. Las principales consecuencias incluyen:

1. **Escalamiento de privilegios**: Los atacantes pueden obtener privilegios de administrador en los sistemas afectados, lo que les permite tomar control completo sobre los dispositivos comprometidos, ejecutar comandos arbitrarios y modificar configuraciones críticas.
2. **Acceso no autorizado a datos sensibles**: Una vez que el atacante obtiene privilegios elevados, puede acceder a datos sensibles o confidenciales, como credenciales de usuario, información financiera, registros personales de clientes, y otros datos críticos almacenados en las plataformas vulnerables.
3. **Compromiso de la infraestructura de TI**: La explotación de esta vulnerabilidad puede permitir a los atacantes moverse lateralmente dentro de la red, afectando otros sistemas y aplicaciones conectados, lo que incrementa el alcance del ataque y permite comprometer más activos dentro de la infraestructura de TI.
4. **Interrupciones operacionales**: Los atacantes pueden interrumpir servicios clave o comprometer la disponibilidad de sistemas críticos, afectando las operaciones diarias de la organización. Esto puede incluir fallos en la infraestructura de TI, pérdida de acceso a aplicaciones esenciales o paralización de sistemas.

5. **Riesgo regulatorio y reputacional**: Si los atacantes exfiltran o manipulan datos sensibles, la organización puede enfrentarse a sanciones regulatorias bajo normativas como el GDPR, Ley 1581 de 2012 (Colombia) o similares, además de un impacto reputacional significativo por no proteger adecuadamente la información confidencial.
6. **Acceso persistente y evasión**: Una vez que los atacantes obtienen acceso mediante la explotación de estas vulnerabilidades, pueden instalar backdoors u otros mecanismos de persistencia, lo que les permite mantener el control sobre el sistema comprometido incluso después de que las acciones correctivas hayan comenzado.

Modo de explotación del ataque

La cadena de ataque de las vulnerabilidades **CVE-2026-32201 y CVE-2026-33825** sigue un conjunto de fases claramente definidas, que permiten a los atacantes explotar estas vulnerabilidades para obtener acceso no autorizado y escalar privilegios en los sistemas afectados. A continuación, se detallan las fases del ataque:

Fase 1 – Identificación de sistemas vulnerables

El atacante comienza identificando los sistemas que utilizan versiones vulnerables de Microsoft Defender o productos relacionados. Esto se puede realizar mediante técnicas de escaneo de redes o aprovechando vulnerabilidades ya conocidas en el sistema para obtener acceso inicial a los dispositivos o redes afectadas.

Fase 2 – Explotación de la vulnerabilidad

Una vez identificado un sistema vulnerable, el atacante explota CVE-2026-32201 o CVE-2026-33825 para aprovechar una debilidad en la validación de datos o en la gestión de privilegios de Microsoft Defender. Esto permite al atacante escalar privilegios y obtener acceso a niveles elevados del sistema sin necesidad de autenticación adicional.

Fase 3 – Escalado de privilegios

En esta fase, el atacante obtiene privilegios elevados en el sistema comprometido. Esto le permite tomar el control completo del dispositivo afectado, ejecutar comandos arbitrarios y acceder a configuraciones críticas que normalmente estarían protegidas por controles de seguridad.

Fase 4 – Comando y control (C2)

Una vez que el atacante ha ganado acceso y control del sistema, establece una comunicación persistente con el servidor de comando y control (C2). Este canal permite al atacante enviar comandos adicionales y obtener información exfiltrada del sistema afectado. La comunicación puede ser mantenida para asegurar el control continuo y el acceso no autorizado.

Fase 5 – Exfiltración de datos o movimiento lateral

Con el acceso al sistema, el atacante puede exfiltrar datos sensibles o moverse lateralmente dentro de la red de la organización, comprometiendo otros sistemas conectados y aumentando el alcance del ataque. Esto podría incluir credenciales de usuario, información financiera, o cualquier dato confidencial almacenado en el sistema.

Fase 6 – Evasión de detección

Los atacantes implementan técnicas de evasión para ocultar su actividad maliciosa. Esto puede incluir la eliminación de registros de actividad o el uso de herramientas de ofuscación para evitar la detección por soluciones de seguridad y mantener el control sin ser detectados durante un largo período.

Vulnerabilidades asociadas

Las vulnerabilidades CVE-2026-32201 y CVE-2026-33825 no dependen de un solo fallo de software, sino que están relacionadas con la gestión inadecuada de privilegios y deficiencias en la validación de datos en varios productos de Microsoft Defender. Estas vulnerabilidades pueden ser explotadas para escalar privilegios y obtener acceso a sistemas sin autenticación adecuada. A continuación, se detallan algunas de las vulnerabilidades y debilidades relacionadas:

1. **Falta de validación adecuada de datos de entrada**: En las vulnerabilidades CVE-2026-32201 y CVE-2026-33825, el software no valida correctamente los datos de entrada proporcionados por los usuarios o aplicaciones. Esto permite a los atacantes enviar datos manipulados, lo que desencadena fallos de seguridad que pueden ser explotados para obtener privilegios elevados.
2. **Gestión débil de privilegios en Microsoft Defender:** La vulnerabilidad permite que los atacantes eludan los controles de seguridad de Microsoft Defender, ganando acceso a privilegios de administrador en sistemas afectados. La falta de controles efectivos para la gestión de privilegios en ciertas configuraciones de Microsoft Defender permite a los atacantes obtener privilegios sin una verificación adecuada.

3. **Abuso de la confianza en el sistema operativo:** Estas vulnerabilidades se aprovechan del hecho de que Microsoft Defender se confía en las configuraciones predeterminadas de seguridad de Windows, que no previenen completamente el escenario de escalada de privilegios. Los atacantes pueden aprovechar la confianza en los procesos legítimos para eludir la detección y ganar acceso privilegiado a los sistemas comprometidos.
4. **Falta de protección en procesos clave**: A pesar de las actualizaciones de seguridad en Microsoft Defender, los atacantes pueden explotar estas vulnerabilidades para modificar o eludir procesos clave, lo que hace que los controles de seguridad se vean comprometidos y reduce la capacidad de respuesta ante incidentes.

Recomendaciones de detección y mitigación

Para mitigar los riesgos asociados con las vulnerabilidades CVE-2026-32201 y CVE-2026-33825 en Microsoft Defender, las organizaciones deben aplicar medidas de detección proactiva y mitigación para evitar que estas vulnerabilidades sean explotadas activamente. A continuación, se detallan las principales recomendaciones para mejorar la seguridad de los sistemas afectados:

1. **Aplicar las actualizaciones de seguridad inmediatamente**: La primera medida es aplicar las actualizaciones de seguridad proporcionadas por Microsoft para corregir las vulnerabilidades CVE-2026-32201 y CVE-2026-33825. Asegúrese de que Microsoft Defender y otros productos afectados estén actualizados a la última versión disponible, que incluye los parches necesarios para mitigar estos riesgos. Las organizaciones deben establecer un proceso ágil de gestión de parches para asegurar que se apliquen las actualizaciones en tiempo y forma.

2. **Monitoreo de eventos de seguridad**: Realice un monitoreo continuo de los sistemas utilizando plataformas SIEM (gestión de eventos e información de seguridad) y EDR (detección y respuesta de endpoints). Los sistemas deben configurarse para alertar sobre comportamientos anómalos, como intentos de escalada de privilegios y accesos no autorizados. Además, es recomendable auditar los registros de seguridad de Microsoft Defender y otros sistemas críticos para detectar actividades sospechosas.
3. **Revisión de accesos y permisos:** Realice una revisión exhaustiva de los registros de acceso y los permisos de usuario en los sistemas afectados. Verifique que no se hayan realizado cambios no autorizados en las cuentas de administración o que no existan cuentas con privilegios excesivos. Limite los privilegios de acceso a la mínima cantidad necesaria para los usuarios y servicios.
4. **Implementar autenticación multifactor (MFA):** Si aún no se ha implementado, habilite autenticación multifactor (MFA) en todas las cuentas de usuario, especialmente para aquellas con privilegios elevados. La MFA proporcionará una capa adicional de protección y dificultará que los atacantes obtengan acceso incluso si logran comprometer las credenciales de usuario.
5. **Implementar controles de acceso estrictos**: Aplique el principio de menor privilegio en la configuración de cuentas y servicios. Asegúrese de que las aplicaciones que utilizan Microsoft Defender tengan configuraciones de acceso estrictas, limitando los permisos solo a los usuarios y sistemas que realmente los necesiten. Utilice políticas de seguridad para evitar que las cuentas con privilegios elevados sean utilizadas de forma inadecuada.
6. **Evaluación de la infraestructura de TI:** Realice un análisis exhaustivo de la infraestructura de TI para identificar otras posibles vulnerabilidades y puntos de acceso no protegidos. Las auditorías de seguridad regulares, como las pruebas de penetración

y el análisis de configuración de seguridad de los sistemas, ayudarán a descubrir fallos adicionales antes de que puedan ser explotados.

7. **Revisión y fortalecimiento de las políticas de defensa perimetral:** Asegúrese de que los firewalls y sistemas de detección de intrusos (IDS) estén configurados para bloquear comunicaciones no autorizadas y evitar que el tráfico malicioso alcance sistemas sensibles. Esto incluye bloquear accesos a puertos no estándar y filtrar conexiones que provengan de direcciones IP desconocidas o mal clasificadas.
8. **Fortalecimiento de la seguridad de las cuentas de servicio:** Revise y fortalezca las configuraciones de seguridad de las cuentas de servicio utilizadas por Microsoft Defender y otros componentes del sistema. Asegúrese de que estén configuradas de acuerdo con las mejores prácticas de seguridad, como el uso de contraseñas fuertes y la rotación periódica de claves.

Recomendaciones de prevención y mitigación

Para reducir el riesgo de explotación de las vulnerabilidades CVE-2026-32201 y CVE-2026-33825 y fortalecer la seguridad de los sistemas afectados, se recomienda implementar las siguientes medidas preventivas y de mitigación:

1. **Aplicación inmediata de actualizaciones de seguridad:** La acción más crítica es aplicar las actualizaciones de seguridad proporcionadas por Microsoft para corregir las vulnerabilidades. Asegúrese de que todas las instancias de Microsoft Defender estén actualizadas con la última versión disponible, ya que las actualizaciones abordan específicamente CVE-2026-32201 y CVE-2026-33825.
2. **Fortalecimiento de la configuración de acceso y privilegios:** Aplique el principio de menor privilegio para todas las cuentas de usuario, limitando los privilegios administrativos solo a los usuarios que realmente lo necesiten. Realice una revisión de

los permisos de acceso y asegúrese de que no haya cuentas con privilegios excesivos o configuraciones inseguras.

3. **Implementación de autenticación multifactor (MFA):** Implemente autenticación multifactor (MFA) en todos los accesos administrativos y críticos dentro de los sistemas afectados. Esta medida agregará una capa adicional de seguridad que puede prevenir el acceso no autorizado, incluso si un atacante obtiene credenciales comprometidas.
4. **Monitoreo y auditoría continua de los sistemas:** Realice un monitoreo activo de todos los sistemas mediante plataformas SIEM (Security Information and Event Management) y EDR (Endpoint Detection and Response). Los sistemas deben ser configurados para detectar comportamientos anómalos relacionados con la explotación de privilegios elevados, como intentos de escalada de privilegios o cambios no autorizados en los accesos a configuraciones críticas.
5. **Revisión de la configuración de Microsoft Defender:** Asegúrese de que Microsoft Defender esté configurado adecuadamente para detectar actividades sospechosas. Revise las políticas de defensa, las configuraciones de antimalware, y habilite las opciones de detección avanzada y protección en tiempo real para reforzar la seguridad.
6. **Fortalecimiento de las políticas de seguridad perimetral:** Proteja los puntos de entrada de la red utilizando firewalls avanzados y sistemas de prevención de intrusos (IPS). Asegúrese de que las soluciones de seguridad perimetral sean capaces de identificar y bloquear conexiones maliciosas, especialmente aquellas que intentan explotar puertos y protocolos no estándar.
7. **Deshabilitar servicios no esenciales:** Revise y deshabilite cualquier servicio no esencial dentro de Microsoft Defender o en el sistema operativo en general, para reducir la superficie de ataque. La desactivación de servicios innecesarios ayuda a minimizar la posibilidad de que los atacantes encuentren puntos débiles.

8. **Auditoría y evaluación de la infraestructura de TI:** Realice auditorías periódicas de seguridad de toda la infraestructura de TI para identificar vulnerabilidades adicionales y configuraciones inseguras. La implementación de pruebas de penetración y evaluaciones regulares de vulnerabilidades ayudará a mantener los sistemas actualizados y seguros frente a amenazas conocidas.
9. **Capacitación y concientización en seguridad cibernética:** Proporcione capacitación regular sobre seguridad cibernética a todos los empleados, especialmente aquellos que tienen acceso a sistemas críticos o que gestionan Microsoft Defender. Concientizar sobre prácticas de seguridad y las amenazas emergentes es esencial para prevenir incidentes de seguridad.
10. **Revisión de la cadena de suministro de software:** Asegúrese de que los sistemas afectados cuenten con software confiable y certificado, evitando la instalación de aplicaciones de terceros no verificadas. Las vulnerabilidades en la cadena de suministro de software pueden ser una vía de entrada para los atacantes, por lo que es crucial aplicar prácticas de seguridad robustas en este sentido.

Recomendaciones de respuesta ante compromiso

En caso de que se confirme la explotación de las vulnerabilidades CVE-2026-32201 y CVE-2026-33825 en Microsoft Defender, las organizaciones deben seguir los siguientes pasos para contener el incidente, mitigar el daño y restaurar la seguridad de los sistemas afectados:

1. **Aislamiento inmediato de sistemas comprometidos:** Desconecte los sistemas afectados de la red de inmediato para evitar la propagación del ataque. Es importante no apagar los dispositivos afectados para preservar la evidencia volátil y permitir un análisis forense adecuado.

2. **Aplicación de parches de seguridad**: Aplique de manera urgente las actualizaciones de seguridad proporcionadas por Microsoft para corregir las vulnerabilidades CVE-2026-32201 y CVE-2026-33825. Asegúrese de que Microsoft Defender y otros productos de seguridad estén actualizados con las versiones más recientes, que corrigen las vulnerabilidades y previenen futuros intentos de explotación.
3. **Revisión de accesos y privilegios:** Realice una revisión exhaustiva de los registros de acceso y los permisos de usuario en los sistemas comprometidos. Verifique que no se hayan realizado cambios no autorizados en las cuentas de administración ni en los privilegios de acceso. Restablezca las contraseñas y otras credenciales comprometidas de inmediato.
4. **Eliminación de malware y herramientas de explotación:** Identifique y elimine cualquier herramienta maliciosa o backdoor que haya sido instalada por los atacantes. Realice un análisis completo de todos los sistemas afectados para detectar y eliminar cualquier componente adicional del ataque.
5. **Monitoreo y análisis forense:** Realice un análisis forense de los sistemas afectados para determinar el alcance del ataque. Esto incluye la recolección de logs de seguridad, imágenes de disco, y datos de memoria RAM para entender cómo se llevó a cabo la explotación y qué datos pudieron haber sido comprometidos.
6. **Revocación de credenciales:** Revise y revogue las credenciales de usuario que hayan sido utilizadas en los sistemas comprometidos. Asegúrese de que las credenciales de los administradores y otros usuarios privilegiados estén protegidas y no se hayan visto comprometidas durante el ataque.
7. **Restauración desde copias de seguridad:** Si los datos comprometidos no pueden ser restaurados de manera segura, considere la restauración de los sistemas desde copias

de seguridad verificadas que no hayan sido afectadas. Asegúrese de que las copias de seguridad estén libres de malware y actualizadas.

8. **Revisión de las políticas de seguridad:** Una vez que el incidente esté contenido, revise las políticas de seguridad y los procedimientos de respuesta a incidentes. Asegúrese de que las medidas de seguridad preventivas, como la autenticación multifactor (MFA), la gestión de parches y la revisión de privilegios, estén implementadas de manera más estricta.
9. **Notificación a las autoridades:** Si el ataque ha comprometido datos sensibles, como información personal o confidencial, notifíquelo a las autoridades reguladoras correspondientes, como el CSIRT o la Superintendencia de Industria y Comercio (en el caso de Colombia). Asegúrese de cumplir con las regulaciones de privacidad y protección de datos, como el GDPR o la Ley 1581 de 2012.
10. **Documentación del incidente y lecciones aprendidas:** Documente todos los pasos seguidos durante el incidente de seguridad y las medidas tomadas. Esta documentación será clave para futuras auditorías y para mejorar los planes de respuesta a incidentes de la organización.

Conclusiones

Las vulnerabilidades CVE-2026-32201 y CVE-2026-33825 en Microsoft Defender representan un riesgo significativo para la seguridad de los sistemas que dependen de esta herramienta crítica de protección. Al ser explotadas activamente por atacantes, estas vulnerabilidades permiten escalada de privilegios y acceso no autorizado a sistemas y datos sensibles, lo que puede tener consecuencias devastadoras para las organizaciones afectadas.

Alerta Vulnerabilidad
Vulnerabilidades CVE-2026-32201 y CVE-2026-33825 Microsoft

CSIRTSALUD-AV-20260430-43 **TLP: CLEAR**

La urgencia de aplicar los parches de seguridad proporcionados por Microsoft no puede subestimarse, ya que las vulnerabilidades son utilizadas por actores maliciosos para comprometer la confidencialidad, integridad y disponibilidad de los sistemas afectados. La CISA ha incluido estas vulnerabilidades en su Catálogo de Vulnerabilidades Explotadas, lo que subraya la necesidad de una respuesta inmediata para mitigar los riesgos de explotación.

Las organizaciones deben actuar sin demora, aplicando las actualizaciones necesarias, revisando sus sistemas y configuraciones de seguridad, y mejorando sus estrategias de defensa en profundidad para protegerse frente a futuras amenazas. Además, el fortalecimiento de las políticas de acceso y autenticación, así como la implementación de medidas de detección y monitoreo proactivo, son esenciales para asegurar que las vulnerabilidades no sean aprovechadas por los atacantes.

En resumen, la explotación de CVE-2026-32201 y CVE-2026-33825 resalta la necesidad de mantener los sistemas actualizados y reforzar las estrategias de seguridad para proteger adecuadamente los datos y las infraestructuras críticas frente a amenazas cada vez más sofisticadas.

Fuentes:

CISA – CISA Adds One Known Exploited Vulnerability to Catalog. Disponible en: https://www.cisa.gov/news-events/alerts/2026/04/22/cisa-adds-one-known-exploited-vulnerability-catalog

Microsoft Security Response Center (MSRC) – Microsoft April 2026 Monthly Rollup - AV26-352. Disponible en: https://www.cyber.gc.ca/en/alerts-advisories/microsoft-security-advisory-april-2026-monthly-rollup-av26-352

TechRadar – CISA puts US government agencies on two-week deadline to patch Microsoft Defender BlueHammer zero-day exploit. Disponible en: https://www.techradar.com/pro/security/cisa-puts-us-government-agencies-on-two-week-deadline-to-patch-microsoft-defender-bluehammer-zero-day-exploit

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.