

Alerta ID:	129
Fecha del reporte:	06/08/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidad en macOS permite acceso a información sensible mediante conexiones VNC
Herramienta de detección	N/A
Activos involucrados:	Equipos macOS con los servicios de Compartir pantalla o Gestión remota habilitados.
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del sector salud sobre la vulnerabilidad de alta severidad identificada como **CVE-2026-43760**, presente en determinadas versiones y configuraciones de macOS. Su explotación podría permitir que un atacante con acceso mediante una contraseña VNC realice operaciones no autorizadas sobre el sistema y acceda a información sensible.

Esta alerta busca orientar la identificación de los equipos potencialmente afectados, la instalación oportuna de las actualizaciones de seguridad publicadas por Apple y la aplicación de medidas preventivas sobre los servicios de acceso remoto, con el fin de reducir el riesgo de accesos no autorizados, alteración de configuraciones y afectación de la información institucional.

Descripción:

Apple corrigió una vulnerabilidad en el componente **Screen Sharing Server** de macOS, utilizado por las funciones Compartir pantalla y Gestión remota. La falla se relaciona con controles de acceso insuficientes durante determinadas operaciones realizadas mediante el protocolo VNC.

La vulnerabilidad afecta principalmente a los equipos que tienen habilitado el servicio de acceso remoto y utilizan la opción heredada **“Los visores VNC pueden controlar la pantalla**

mediante contraseña". Para aprovecharla, el atacante debe poder conectarse al servicio y conocer la contraseña VNC configurada; no es suficiente con que el equipo ejecute una versión vulnerable de macOS.

De acuerdo con la investigación técnica divulgada, una conexión VNC autenticada podría efectuar operaciones sobre archivos con permisos superiores a los esperados. Esta condición podría facilitar el acceso a información sensible y, dependiendo de la configuración del sistema y de las acciones realizadas, permitir modificaciones en ubicaciones protegidas.

Los investigadores demostraron que el comportamiento podía utilizarse para crear archivos con privilegios elevados y modificar la configuración del sistema. Esto aumentaría el impacto potencial hasta permitir la ejecución de comandos con privilegios de administrador. Apple describe oficialmente el impacto de CVE-2026-43760 como la posibilidad de que una aplicación acceda a información sensible del usuario.

La vulnerabilidad fue corregida mediante el fortalecimiento de los controles y restricciones de acceso en el componente afectado. Las entidades deben actualizar los equipos y verificar que los servicios de acceso remoto únicamente permanezcan habilitados cuando sean necesarios.

Vulnerabilidad con evidencia de explotación

La vulnerabilidad **CVE-2026-43760** afecta el componente Screen Sharing Server de macOS, utilizado por las funciones Compartir pantalla y Gestión remota. La falla está relacionada con controles de acceso insuficientes durante determinadas operaciones realizadas mediante conexiones VNC.

La vulnerabilidad presenta una severidad alta y cuenta con una puntuación CVSS de **8,6 sobre 10**, de acuerdo con la información técnica divulgada públicamente. Apple corrigió la falla mediante la incorporación de restricciones adicionales de acceso en el componente afectado.

Descripción:

La vulnerabilidad podría ser aprovechada cuando un equipo tiene habilitada la función Compartir pantalla o Gestión remota y permite que los visores VNC controlen la pantalla mediante una contraseña.

Para intentar su explotación, el atacante debe tener conectividad con el servicio VNC y conocer la contraseña configurada. No requiere las credenciales de una cuenta de macOS ni la intervención posterior del usuario una vez establecida la conexión.

De acuerdo con la investigación divulgada, una conexión VNC autenticada podría efectuar operaciones sobre archivos con privilegios superiores a los esperados. Los investigadores demostraron que esta condición podía utilizarse para crear archivos en ubicaciones protegidas y modificar la configuración del sistema.

Apple describe oficialmente el impacto de CVE-2026-43760 como la posibilidad de que una aplicación acceda a información sensible del usuario. La investigación técnica señala que, bajo la configuración vulnerable, el acceso indebido a archivos también podría utilizarse para obtener privilegios administrativos.

Impacto:

La explotación exitosa de la vulnerabilidad podría comprometer la confidencialidad y la integridad de la información almacenada en el equipo afectado. Dependiendo de la configuración del sistema y de los permisos obtenidos, un atacante podría:

- Acceder a información sensible del usuario.
- Crear o modificar archivos en ubicaciones protegidas.
- Alterar configuraciones de seguridad.
- Obtener privilegios administrativos sobre el equipo.
- Instalar programas o mecanismos de persistencia.
- Utilizar el dispositivo comprometido para acceder a otros recursos institucionales.
- Exponer información personal, administrativa, clínica o asistencial.

El impacto puede ser mayor en equipos accesibles desde Internet, dispositivos que utilicen contraseñas VNC débiles o reutilizadas y sistemas conectados a redes que no cuenten con una segmentación adecuada.

Estado de explotación:

A la fecha de elaboración de esta alerta no se ha identificado evidencia pública confirmada de explotación activa de **CVE-2026-43760** en ataques reales. La información disponible corresponde a una investigación de seguridad en la que se demostró técnicamente la posibilidad de aprovechar la vulnerabilidad.

La existencia de una demostración técnica no debe confundirse con una campaña activa de explotación. Sin embargo, la divulgación de los detalles de la falla podría facilitar que actores maliciosos desarrollen o adapten mecanismos para aprovecharla en equipos que permanezcan sin actualizar.

Por esta razón, las entidades deben priorizar la identificación de dispositivos con la configuración vulnerable, instalar las actualizaciones publicadas por Apple y restringir temporalmente los servicios de acceso remoto cuando la actualización no pueda aplicarse de manera inmediata.

Productos y versiones afectadas

La vulnerabilidad **CVE-2026-43760** afecta el componente Screen Sharing Server de macOS. De acuerdo con los avisos de seguridad publicados por Apple, la falla fue corregida en las siguientes versiones:

- macOS Tahoe 26.6
- macOS Sonoma 14.8.8

En consecuencia, deben considerarse potencialmente afectadas las versiones anteriores de macOS Tahoe y macOS Sonoma que no cuenten con estas actualizaciones de seguridad. El riesgo de explotación se concentra principalmente en los equipos que, además de utilizar una versión vulnerable, presentan alguna de las siguientes condiciones:

- Tienen habilitada la función Compartir pantalla.
- Tienen habilitada la función Gestión remota.
- Permiten que los visores VNC controlen la pantalla mediante una contraseña.
- Exponen el servicio VNC a Internet o a redes no confiables.

- Utilizan contraseñas VNC débiles, reutilizadas o potencialmente comprometidas.

La presencia de una versión vulnerable no implica por sí sola que el equipo pueda ser explotado de forma inmediata. Para materializar el ataque deben encontrarse habilitadas las funciones relacionadas con VNC y el atacante debe conocer la contraseña configurada.

Activos con mayor exposición

Los equipos con mayor nivel de exposición son aquellos que ejecutan una versión vulnerable de macOS y mantienen habilitados servicios de acceso remoto mediante VNC. La prioridad de revisión debe establecerse considerando la accesibilidad del equipo, la configuración aplicada y la sensibilidad de la información que procesa.

Se deben priorizar los siguientes activos:

- Equipos Mac con Compartir pantalla o Gestión remota habilitados.
- Dispositivos que permiten el control mediante una contraseña VNC.
- Equipos cuyo servicio VNC es accesible directamente desde Internet.
- Dispositivos conectados a redes de terceros o segmentos con controles de acceso limitados.
- Equipos utilizados por administradores, personal directivo o usuarios con privilegios elevados.
- Dispositivos que almacenan o procesan información personal, clínica, asistencial, financiera o administrativa.
- Equipos desde los cuales se accede a sistemas de información institucionales o servicios críticos.
- Dispositivos que no se encuentran administrados mediante una herramienta centralizada.
- Equipos que no reciben actualizaciones de seguridad periódicas o utilizan versiones de macOS sin soporte.
- Sistemas que emplean contraseñas VNC débiles, compartidas o reutilizadas en otros servicios.

La exposición disminuye cuando el acceso remoto se encuentra deshabilitado, restringido a redes internas autorizadas o protegido mediante VPN, reglas de firewall y controles

adicionales de autenticación. No obstante, estas medidas reducen el riesgo, pero no reemplazan la instalación de las actualizaciones publicadas por Apple.

Consideraciones para el sector salud

En las entidades del sector salud, los equipos con macOS pueden ser utilizados en actividades administrativas, comunicaciones, investigación, telemedicina, diseño, procesamiento de imágenes, soporte técnico y acceso a plataformas institucionales. Algunos de estos dispositivos pueden almacenar información sensible o mantener sesiones autorizadas en sistemas clínicos, administrativos y asistenciales.

La explotación de la vulnerabilidad podría facilitar el acceso no autorizado a datos personales, información clínica, credenciales institucionales, documentos internos y otros recursos disponibles desde el equipo comprometido. El riesgo aumenta cuando el usuario afectado cuenta con privilegios elevados o tiene acceso a servicios esenciales para la operación de la entidad.

Un atacante también podría utilizar el equipo comprometido como punto de entrada para intentar desplazarse hacia otros sistemas de la red. Por esta razón, la revisión no debe limitarse al dispositivo macOS, sino que debe considerar las conexiones, credenciales y recursos institucionales a los que puede acceder.

Las entidades deben priorizar la actualización de los equipos utilizados en áreas asistenciales, administrativas y de investigación, especialmente cuando procesen información personal o sensible. También deben verificar que las funciones de Compartir pantalla y Gestión remota respondan a una necesidad operativa y cuenten con autorización, seguimiento y controles de acceso adecuados.

La aplicación de la actualización contribuye a proteger la confidencialidad e integridad de la información y a reducir la posibilidad de que un acceso remoto no autorizado afecte la continuidad de los servicios institucionales.

Indicadores de compromiso (IoC) y actividades de detección

A la fecha de elaboración de esta alerta no se han publicado indicadores de compromiso específicos, como direcciones IP, dominios, archivos maliciosos o valores hash, relacionados con la explotación activa de **CVE-2026-43760**.

La ausencia de estos indicadores no impide realizar actividades de verificación. Las entidades deben revisar los registros del sistema operativo, las herramientas de seguridad y los controles de red para identificar comportamientos que puedan estar relacionados con accesos remotos no autorizados.

Se recomienda prestar especial atención a:

- Conexiones VNC inesperadas o realizadas desde direcciones IP desconocidas.
- Tráfico no autorizado hacia el puerto TCP 5900, utilizado habitualmente por VNC.
- Conexiones efectuadas fuera de los horarios establecidos o desde ubicaciones inusuales.
- Intentos reiterados o fallidos de autenticación contra los servicios de acceso remoto.
- Activación no autorizada de Compartir pantalla, Gestión remota o del acceso mediante contraseña VNC.
- Creación o modificación de archivos en directorios protegidos del sistema.
- Cambios inesperados en usuarios, grupos, privilegios o configuraciones administrativas.
- Ejecución de comandos con privilegios elevados que no correspondan a actividades autorizadas.
- Instalación de aplicaciones, servicios, agentes o mecanismos de persistencia desconocidos.
- Alertas generadas por las soluciones EDR/XDR relacionadas con escalamiento de privilegios o manipulación de componentes del sistema.
- Accesos posteriores desde el equipo afectado hacia otros sistemas o servicios institucionales.

Las actividades identificadas deben compararse con los registros de soporte remoto, las ventanas de mantenimiento y los cambios autorizados. Cuando no sea posible justificar una conexión o modificación, la entidad debe conservar las evidencias disponibles e iniciar el procedimiento institucional de análisis y respuesta a incidentes.

Medidas de Prevención



Para reducir el riesgo asociado con **CVE-2026-43760**, las entidades deben mantener actualizados los equipos macOS y limitar el uso de los servicios de acceso remoto a los casos en que exista una necesidad operativa debidamente autorizada.

Se recomienda implementar las siguientes medidas:

- Actualizar los equipos a **macOS Tahoe 26.6**, **macOS Sonoma 14.8.8** o una versión posterior compatible.
- Verificar que la actualización se haya instalado correctamente en todos los equipos identificados.
- Deshabilitar la opción que permite a los visores VNC controlar la pantalla mediante una contraseña.
- Desactivar Compartir pantalla y Gestión remota cuando estas funciones no sean necesarias.
- Restringir las conexiones remotas mediante VPN, reglas de firewall, segmentación de red y listas de direcciones autorizadas.
- Utilizar contraseñas robustas, únicas y administradas de forma segura para los servicios de acceso remoto.
- Cambiar las contraseñas VNC que sean compartidas, reutilizadas o que puedan haber quedado expuestas.
- Limitar los permisos de los usuarios y cuentas utilizados para prestar soporte remoto.
- Mantener activas y actualizadas las soluciones EDR/XDR y los controles de seguridad instalados en los dispositivos.
- Centralizar y conservar los registros relacionados con las conexiones remotas y los cambios administrativos.
- Capacitar al personal de soporte sobre el uso seguro de las herramientas de acceso remoto.

La desactivación de la opción VNC heredada y la restricción de las conexiones reducen la superficie de exposición mientras se realiza la actualización. Sin embargo, estas medidas no sustituyen la instalación de las correcciones publicadas por Apple.

Medidas de detección y mitigación

Las entidades deben realizar una revisión de los equipos macOS para identificar las versiones instaladas y determinar cuáles tienen habilitadas las funciones Compartir pantalla, Gestión remota o acceso mediante contraseña VNC.

Como parte de esta revisión, se recomienda:

- Elaborar o actualizar el inventario de equipos macOS de la entidad.
- Identificar los dispositivos que ejecutan versiones anteriores a macOS Tahoe 26.6 o macOS Sonoma 14.8.8.
- Verificar cuáles equipos tienen habilitados servicios de acceso remoto mediante VNC.
- Determinar si estos servicios son accesibles desde Internet, redes de terceros o segmentos no autorizados.
- Revisar las reglas de firewall y restringir el puerto TCP 5900 a los orígenes estrictamente necesarios.
- Consultar los registros de conexiones remotas para identificar accesos atípicos o no autorizados.
- Verificar la creación o modificación reciente de archivos en ubicaciones protegidas.
- Revisar cambios en cuentas, privilegios, servicios y configuraciones administrativas.
- Correlacionar los hallazgos con las alertas generadas por las soluciones EDR/XDR, SIEM y monitoreo de red.

Cuando un equipo no pueda actualizarse de manera inmediata, se debe deshabilitar el acceso mediante contraseña VNC. Si Compartir pantalla o Gestión remota no son indispensables, estos servicios deben permanecer desactivados hasta que se instale la actualización correspondiente.

Si el acceso remoto es necesario para la operación, debe limitarse temporalmente mediante VPN, segmentación de red, reglas de firewall y direcciones IP autorizadas. También se deben cambiar las contraseñas VNC y supervisar las conexiones hasta completar la actualización.

Respuesta ante una posible explotación

Cuando se identifiquen conexiones VNC sospechosas, modificaciones no autorizadas o señales de escalamiento de privilegios, la entidad debe activar su procedimiento de gestión de incidentes de seguridad.

Se recomienda ejecutar las siguientes acciones:

- Aislar de la red el equipo potencialmente comprometido para evitar accesos adicionales o desplazamientos hacia otros sistemas.
- Deshabilitar Compartir pantalla, Gestión remota y el acceso mediante contraseña VNC.
- Bloquear las direcciones IP relacionadas con la actividad sospechosa, cuando hayan podido identificarse.
- Preservar los registros, archivos y demás evidencias necesarias para el análisis técnico.
- Identificar las cuentas, contraseñas, certificados, sesiones y recursos institucionales que pudieron quedar expuestos.
- Cambiar las credenciales comprometidas o utilizadas desde el equipo afectado y revocar las sesiones activas.
- Revisar la creación o modificación de usuarios, grupos, archivos, servicios, tareas programadas y mecanismos de persistencia.
- Analizar las conexiones realizadas desde el equipo hacia otros activos de la entidad.
- Verificar si se produjo acceso, modificación, extracción o eliminación de información institucional.
- Examinar otros dispositivos con configuraciones similares para determinar si presentan señales relacionadas.
- Aplicar la actualización de seguridad antes de restablecer el acceso remoto o reincorporar el equipo a la red.
- Restaurar el sistema desde una fuente confiable cuando no sea posible garantizar su integridad.
- Documentar los hallazgos, las decisiones adoptadas y las acciones ejecutadas durante la atención del incidente.
- Reportar el evento al equipo institucional responsable de seguridad digital y seguir los canales de notificación establecidos.

El restablecimiento del equipo debe realizarse únicamente después de confirmar que la vulnerabilidad fue corregida, las credenciales potencialmente comprometidas fueron renovadas y no permanecen mecanismos de acceso no autorizado.

Fuentes:

- <https://support.apple.com/100100>
- <https://support.apple.com/en-us/128067>

- <https://support.apple.com/en-us/128072>
- <https://securityonline.info/apple-bug-bounty-ai/>
- <https://www.techradar.com/pro/security/a-potentially-dangerous-macos-security-flaw-went-unreported-due-to-apple-being-deluged-by-ai-slop-bug-reports>

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 **contacto@csirtsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.