Alerta ID:	098
Fecha del reporte:	11/05/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades en el **kernel de Linux**
Herramienta de detección	N/A
Activo involucrado:	Sistemas Linux
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la identificación de una nueva amenaza crítica, **Dirty Frag**, que explota vulnerabilidades en el **kernel de Linux**. Este fallo permite la escalación de privilegios, lo que podría resultar en acceso no autorizado a sistemas críticos, comprometiendo la confidencialidad, integridad y disponibilidad de los datos de pacientes y afectando las operaciones clave en el sector salud.

El propósito de esta alerta es que las organizaciones del sector salud validen si están utilizando alguna distribución del **kernel de Linux** afectada, ya sea en infraestructura propia, en ambientes en la nube, a través de servicios tercerizados o en soluciones integradas a sus procesos misionales. Esta validación debe incluir la revisión de sus inventarios tecnológicos, plataformas de integración de datos clínicos, sistemas de registro de pacientes y otros componentes relacionados con la gestión de información crítica en salud.

.

Descripción:

La vulnerabilidad Dirty Frag es una brecha crítica en el kernel de Linux que permite a un atacante local obtener acceso con privilegios de root. Esta explotación se aprovecha de fallos en el manejo de memoria, lo que permite la escalación de privilegios sin necesidad de autenticación. Afecta a todas las principales distribuciones de Linux, incluidas Ubuntu, Fedora, CentOS, entre otras.

Este fallo puede impactar servidores Linux que utilicen versiones vulnerables del kernel, afectando a organizaciones del sector salud que empleen infraestructura propia o servicios en la nube con estos sistemas operativos.

Actualmente, no hay un parche disponible, y el exploit fue revelado recientemente. Esto hace que sea una vulnerabilidad de tipo zero-day, sin una solución oficial para mitigarla aún. Es crucial que las organizaciones implementen medidas de mitigación temporal para evitar que los atacantes puedan explotar esta vulnerabilidad.

Consecuencias de la explotación

La explotación de la vulnerabilidad Dirty Frag en el kernel de Linux puede tener varias consecuencias graves para las organizaciones del sector salud que empleen sistemas basados en Linux. Las consecuencias incluyen:

1. Acceso no autorizado a sistemas críticos: La vulnerabilidad permite a un atacante local, sin necesidad de autenticación, obtener privilegios de root en el sistema. Esto implica que el atacante podría tomar control completo de los servidores afectados, afectando la integridad y disponibilidad de los Sistemas de Información Hospitalaria (SIH) y otros

componentes críticos de infraestructura tecnológica, como bases de datos de pacientes y plataformas de integración de datos clínicos.

2. Riesgo para la confidencialidad de los datos de los pacientes: Al obtener privilegios elevados, un atacante podría acceder a información sensible, como datos médicos personales de los pacientes, historiales médicos, diagnósticos, e información financiera relacionada con los servicios de salud. Este tipo de acceso sin control compromete la confidencialidad de la información, lo cual representa una violación grave de la privacidad y de las regulaciones de protección de datos (por ejemplo, la Ley General de Protección de Datos en Colombia).
3. Interrupción de servicios y operaciones críticas: Con privilegios de root, los atacantes podrían deshabilitar servicios, alterar configuraciones de infraestructura o incluso destruir datos esenciales. Esto podría interrumpir el funcionamiento normal de los sistemas de salud, afectando la prestación de servicios a los pacientes, el acceso a historiales médicos o la gestión de recursos médicos. Tal interrupción podría afectar directamente la atención de los pacientes, lo que constituye un riesgo para la seguridad de las personas.
4. Pérdida de confianza y reputación: La explotación de esta vulnerabilidad podría afectar gravemente la reputación de las organizaciones de salud involucradas. La pérdida de confianza de los pacientes y socios comerciales es una consecuencia que podría tener efectos a largo plazo, especialmente en un sector tan crítico como el de la salud. La falta de protección de los datos sensibles podría resultar en sanciones regulatorias, así como en la perdida de pacientes.
5. Impacto económico: Los costos de remediar una brecha de seguridad, incluyendo la recuperación de datos y el cierre de la vulnerabilidad, pueden ser elevados. Además, las multas regulatorias relacionadas con la violación de leyes de protección de datos o de normas sectoriales pueden aumentar significativamente los costos. El impacto económico también puede venir de la interrupción operativa, el tiempo de inactividad de los sistemas, y la compensación a los afectados.

6. Posible acceso a redes internas y otros sistemas: Una vez que los atacantes logran obtener privilegios de root, tienen el potencial de moverse lateralmente dentro de la infraestructura de la organización. Esto podría permitirles infectar otros sistemas dentro de la red, accediendo a plataformas de servicios en la nube, servidores de bases de datos, sistemas de gestión de usuarios, y otras aplicaciones críticas que forman parte del ecosistema tecnológico de la organización.

Modo de explotación del ataque

El modo de explotación de la vulnerabilidad Dirty Frag permite a un atacante local escalar privilegios en un sistema basado en Linux sin necesidad de autenticarse previamente. A continuación, se describe cómo se lleva a cabo este tipo de ataque:

Requisito inicial: acceso local:

El atacante debe tener acceso local al sistema vulnerable, ya sea físicamente en el servidor o mediante algún tipo de acceso remoto (por ejemplo, un usuario estándar con privilegios limitados).

Explotación de la vulnerabilidad del manejo de memoria:

La vulnerabilidad se encuentra en la gestión de memoria dentro del kernel de Linux. El atacante puede aprovechar un fallo específico en el manejo de ciertos módulos del kernel, como los relacionados con el manejo de conexiones de red y procesos de seguridad. Al abusar de este fallo, el atacante puede sobrescribir áreas de memoria que normalmente están restringidas.

Escalación de privilegios:

Una vez que el atacante explota esta falla de memoria, puede escalar sus privilegios y obtener acceso a nivel root (administrador del sistema), lo que le otorga control total sobre el sistema

afectado. Esto permite al atacante ejecutar comandos arbitrarios con privilegios elevados, lo que no sería posible con los privilegios estándar de un usuario común.

Acciones post-explotación:

- **Acceso completo a sistemas y datos críticos**: El atacante, ahora con privilegios de **root**, puede acceder a datos sensibles, como registros médicos, datos financieros y otro tipo de información crítica almacenada en el sistema.
- **Instalación de malware o herramientas de persistencia**: El atacante puede instalar **malware** o herramientas de administración remota para mantener el control sobre el sistema a largo plazo, incluso si el sistema es reiniciado o parchado parcialmente.
- **Desactivación de servicios y ocultación de rastros**: El atacante puede deshabilitar sistemas de monitoreo o borrar registros de acceso, lo que dificulta la detección y recuperación posterior del incidente.

Explotación en masa y movimiento lateral:

Dado que el ataque explota una vulnerabilidad del kernel, el atacante tiene la capacidad de propagarse dentro de una red de sistemas conectados. Este tipo de vulnerabilidad podría infectar múltiples servidores y permitir al atacante moverse lateralmente a través de diferentes sistemas, aumentando el alcance del ataque.

Vulnerabilidades asociadas

Fallas en la gestión de memoria del kernel de Linux:

- **Descripción:** La vulnerabilidad Dirty Frag se origina por una mala gestión de memoria en el kernel de Linux, que puede permitir a los atacantes sobrescribir áreas de memoria

restringidas, afectando la integridad del sistema. Este tipo de fallo generalmente está relacionado con problemas en la gestión de buffers, que son comunes en muchas vulnerabilidades de escalación de privilegios.

- **Impacto:** La explotación de esta vulnerabilidad permite la ejecución de código arbitrario con privilegios de root y el acceso a áreas de memoria críticas.

Exposición de interfaces de red no seguras:

- **Descripción:** La explotación de Dirty Frag a menudo se realiza a través de módulos de red como esp4, esp6, y rxrpc, los cuales están involucrados en la gestión de conexiones seguras y la seguridad de la red (por ejemplo, IPSec VPN). Si estos módulos no están correctamente configurados o actualizados, los atacantes pueden aprovechar su debilidad para escalar privilegios en el sistema.
- **Impacto:** Los sistemas que utilizan VPNs o conexiones de red cifradas son especialmente vulnerables si estos módulos no están adecuadamente protegidos o parcheados.

Fallas de seguridad en la autenticación y gestión de acceso:

- **Descripción:** En sistemas donde la autenticación no es fuerte o la gestión de privilegios no se realiza correctamente, un atacante podría aprovechar la escalación de privilegios proporcionada por Dirty Frag para ganar acceso completo a sistemas sin necesidad de autenticarse correctamente.

- **Impacto:** Un atacante podría eludir métodos de autenticación y obtener acceso a los sistemas de gestión de usuarios, bases de datos y otros componentes críticos, lo que comprometería la seguridad de la infraestructura.

Vulnerabilidad en la función de actualización del kernel:

- **Descripción:** Otra posible vulnerabilidad asociada a Dirty Frag está en el proceso de actualización del kernel de Linux. Si el kernel no se actualiza adecuadamente o se aplica un parche incorrecto, las versiones anteriores del kernel siguen siendo vulnerables.
- **Impacto:** Si las organizaciones no gestionan adecuadamente las actualizaciones de seguridad del kernel, los atacantes podrían seguir explotando la vulnerabilidad incluso después de un intento de mitigación, lo que prolonga el riesgo de explotación.

Vulnerabilidad de persistencia y control a largo plazo:

- **Descripción:** La persistencia del atacante en el sistema, una vez que obtiene acceso root, podría ser otra vulnerabilidad asociada. Los atacantes pueden instalar rootkits, backdoors, o modificar archivos críticos del sistema para asegurar el control a largo plazo sobre el sistema afectado.
- **Impacto:** Este tipo de vulnerabilidad es especialmente peligrosa, ya que una vez comprometido un sistema, los atacantes podrían seguir accediendo a él sin ser detectados durante largos períodos, dificultando la detección y la remediación

Relación con otras vulnerabilidades en sistemas Linux:

- Además de las vulnerabilidades específicas de Dirty Frag, existen fallos comunes en distribuciones de Linux que están relacionados, como:
- Vulnerabilidades en el manejo de buffers: Estas vulnerabilidades pueden ser exploradas por atacantes para sobrescribir espacios de memoria y ejecutar código malicioso. Muchos ataques de escalación de privilegios comienzan explotando este tipo de vulnerabilidad.
- Problemas en la configuración de redes VPN: Configuraciones débiles en la seguridad de conexiones de red o el mal manejo de módulos como ESP y RXRPC puede facilitar los intentos de explotación.
- Fallas en las versiones antiguas de sistemas operativos: Muchas de las vulnerabilidades conocidas en Linux se deben a que las versiones anteriores de los kernels o distribuciones no se mantienen correctamente, dejando puertas abiertas para los ataques.

Recomendaciones de detección y mitigación

Para detectar y mitigar eficazmente la amenaza representada por **Dirty Frag**, es fundamental que las entidades implementen medidas de seguridad avanzadas, orientadas a la identificación de comportamientos maliciosos y a la protección de sus sistemas. A continuación, se presentan algunas recomendaciones clave:

1. **Mitigación temporal:** Deshabilitar los módulos vulnerables esp4, esp6, y rxrpc hasta que se libere un parche.

Estos módulos están relacionados con la funcionalidad VPN y AFS, y su deshabilitación podría afectar ciertos servicios.

2. **Revisión de infraestructura:** Las organizaciones deben realizar una revisión inmediata de sus servidores Linux y verificar si están utilizando versiones vulnerables del kernel.

Es importante identificar si sus sistemas operativos basados en Linux están actualizados a las últimas versiones disponibles y aplicar las actualizaciones cuando sea posible.

3. **Monitoreo constante:** Activar alertas de seguridad y monitorear logs de los sistemas afectados para detectar intentos de explotación, especialmente en servicios que operan con privilegios elevados.
4. **Cuentas con privilegios elevados:** Limitar el uso de cuentas con privilegios de root y activar el principio de mínimos privilegios en sistemas afectados

Relación con otras vulnerabilidades en sistemas Linux:

Además de las vulnerabilidades específicas de Dirty Frag, existen fallos comunes en distribuciones de Linux que están relacionados, como:

1. **Vulnerabilidades en el manejo de buffers:** Estas vulnerabilidades pueden ser exploradas por atacantes para sobrescribir espacios de memoria y ejecutar código malicioso. Muchos ataques de escalación de privilegios comienzan explotando este tipo de vulnerabilidad.

2. **Problemas en la configuración de redes VPN:** Configuraciones débiles en la seguridad de conexiones de red o el mal manejo de módulos como ESP y RXRPC puede facilitar los intentos de explotación.
3. **Fallas en las versiones antiguas de sistemas operativos:** Muchas de las vulnerabilidades conocidas en Linux se deben a que las versiones anteriores de los kernels o distribuciones no se mantienen correctamente, dejando puertas abiertas para los ataques.

Recomendaciones de prevención y mitigación

Para mitigar los riesgos asociados con la vulnerabilidad Dirty Frag en el kernel de Linux, es esencial aplicar parches de seguridad de inmediato, deshabilitar módulos vulnerables si no son necesarios, fortalecer la seguridad de las conexiones de red y aplicar principios de mínimos privilegios. Además, las organizaciones deben establecer un sistema de monitoreo activo, realizar auditorías regulares y fomentar la concienciación sobre seguridad dentro de sus equipos

Actualización del Kernel de Linux:

Aplicar parches de seguridad inmediatamente: La actualización del kernel es la medida más eficaz para mitigar las vulnerabilidades como Dirty Frag. Una vez que se publique un parche oficial, es fundamental aplicarlo a la brevedad. Si se está utilizando una distribución de Linux vulnerable, asegúrese de que los repositorios estén configurados correctamente para obtener actualizaciones automáticas.

Deshabilitar los módulos esp4, esp6 y rxrpc:

Si no utiliza estos módulos para VPN o conexiones de red cifradas, desactívelos inmediatamente para mitigar la vulnerabilidad hasta que haya una solución de seguridad disponible.

Fortalecer la seguridad de las VPN:

Si está utilizando servicios de VPN o IPSec, asegúrese de que estén configurados de manera segura y de que los módulos vulnerables no estén activos. Revise las configuraciones de seguridad de las redes internas, especialmente las conexiones de red cifradas y las interfaces de red

Aplique reglas estrictas en el firewall para restringir el acceso remoto y el tráfico de red no autorizado. Utilice firewalls basados en host (como ufw en Ubuntu) para limitar las conexiones entrantes y salientes.

Restringir el uso de cuentas con privilegios elevados:

Limite el uso de cuentas con privilegios root o de administrador. Asegúrese de que solo usuarios autorizados puedan ejecutar tareas críticas. El uso de sudoers debe ser restringido y gestionado cuidadosamente.

Implementar acceso con autenticación multifactor (MFA):

Para sistemas que requieren acceso elevado, utilice autenticación multifactor (MFA) para reducir el riesgo de que los atacantes obtengan acceso a privilegios elevados.

Monitoreo de actividad de red y archivos:

Establezca un sistema de monitoreo para detectar comportamientos inusuales, como accesos no autorizados o cambios inesperados en los archivos críticos del sistema. Herramientas como fail2ban o AIDE (Advanced Intrusion Detection Environment) pueden ayudar a prevenir ataques.

Registros de seguridad (logs):

Configure el sistema para almacenar y revisar los registros de seguridad. Habilite la auditoría de usuarios, la actividad de red y los eventos de acceso con herramientas como auditd.

Auditoría de seguridad regular:

Realice auditorías de seguridad periódicas en sus servidores Linux para identificar posibles vulnerabilidades antes de que puedan ser explotadas. Las herramientas como Lynis pueden ayudar en la auditoría de seguridad de sistemas basados en Linux.

Verificación de integridad de archivos del sistema:

Use herramientas como AIDE para verificar la integridad de los archivos y detectar modificaciones no autorizadas. AIDE genera sumas de comprobación para los archivos clave del sistema y las compara con su estado inicial

Entrenamiento de personal:

Asegúrese de que el personal técnico y los administradores de sistemas estén capacitados sobre las mejores prácticas de seguridad cibernética y sobre cómo identificar y responder a amenazas como Dirty Frag.

Implementación de políticas de seguridad estrictas:

Desarrolle políticas de seguridad claras para el manejo de vulnerabilidades y la gestión de parches.

Recomendaciones de respuesta ante compromiso

Si se sospecha que un sistema ha sido comprometido debido a la explotación de la vulnerabilidad Dirty Frag en el kernel de Linux, es esencial actuar de inmediato para contener el incidente, mitigar los daños y restaurar la seguridad del entorno. A continuación, se describen las acciones clave a seguir:

Aislamiento del Sistema Afectado:

Desconectar de la red: El primer paso es aislar el sistema comprometido desconectándolo de la red para evitar que el atacante se propague o continúe con sus actividades maliciosas. Esto detiene el acceso remoto y evita la propagación lateral a otros sistemas de la red.

Si es posible, apague el sistema afectado de forma segura. Si el apagado no es viable, deshabilite las interfaces de red de forma temporal.

Bloquear puertos de red asociados a la explotación (por ejemplo, puertos utilizados para acceso remoto).

Análisis y Confirmación del Compromiso:

Revisión de registros (logs): Realice una revisión exhaustiva de los registros de seguridad (logs) del sistema para identificar cualquier actividad sospechosa antes y después de la

explotación. Esto puede incluir accesos no autorizados, modificaciones de archivos, o ejecución de comandos con privilegios elevados.

Revisa los logs de acceso y de autenticación (/var/log/auth.log, /var/log/secure en sistemas Linux).

Busca comandos ejecutados con privilegios de root que no hayan sido autorizados, como sudo o cambios en archivos críticos del sistema.

Herramientas de análisis forense:

Utiliza herramientas de análisis forense como **Volatility, chkrootkit** o **rkhunter** para buscar rootkits o cualquier otra señal de persistencia.

Contención del Ataque:

- **Revocar acceso de usuarios comprometidos**: Si se detectan cuentas comprometidas, revocar inmediatamente el acceso de esos usuarios. Cambie las contraseñas de las cuentas afectadas y habilite autenticación multifactor (MFA) si no está configurada.
    - Deshabilitar cuentas de usuarios no autorizados o con privilegios elevados si es necesario.
- **Deshabilitar módulos vulnerables**: Si no se ha realizado previamente, asegúrese de deshabilitar los módulos vulnerables (esp4, esp6, rxrpc) hasta que el sistema esté completamente parcheado y seguro.

Erradicación de la Amenaza:

- **Actualización del kernel**: Una vez que se ha aislado el sistema y se han identificado las señales de compromiso, es necesario actualizar el kernel a una versión segura para cerrar la vulnerabilidad.
    - Actualice el kernel de Linux a la versión más reciente disponible que resuelva el problema de Dirty Frag.
    - Verificar que la actualización del kernel haya sido exitosa con uname -r.
- **Búsqueda y eliminación de backdoors**:

Los atacantes pueden haber instalado **backdoors** o **rootkits** para mantener el acceso al sistema. Realice un análisis forense exhaustivo para identificar y eliminar estos programas maliciosos.

- Ejecute herramientas como **Lynis** o **AIDE** para verificar la integridad del sistema y detectar cualquier archivo comprometido.
- **Eliminar procesos o archivos maliciosos** detectados en el análisis.

Restauración del Sistema:

- **Restaurar desde copias de seguridad**: Si se cuenta con copias de seguridad seguras realizadas antes del compromiso, restaure el sistema a su estado funcional anterior. Asegúrese de que las copias de seguridad no estén comprometidas.
    - Verificar la integridad de las copias de seguridad antes de restaurarlas, para garantizar que no estén infectadas.

- **Reinstalación de sistemas críticos**: Si no se puede confiar en el sistema afectado, considere reinstalar completamente el sistema operativo y las aplicaciones afectadas, asegurándose de aplicar parches de seguridad antes de ponerlo en producción.

Comunicación y Notificación:

- **Notificación interna**: Notifique al equipo de seguridad informática y a la alta dirección sobre el compromiso para coordinar la respuesta, evaluar el impacto y tomar decisiones sobre las acciones adicionales necesarias.
- **Notificación a terceros**: Si el compromiso afecta a datos personales de los pacientes o a información sensible del sector salud, es posible que deba notificar a las autoridades regulatorias de protección de datos, como la SIC (Superintendencia de Industria y Comercio) en Colombia, conforme a la legislación de protección de datos personales.
    - También es importante notificar a cualquier proveedor de servicios de seguridad involucrado, como los de infraestructura en la nube o proveedores de VPN.

Prevención a Largo Plazo:

- **Auditorías periódicas de seguridad**: Después de contener el incidente, realice una auditoría de seguridad más exhaustiva en toda la infraestructura para asegurarse de que no haya más vulnerabilidades críticas.
    - Monitorear logs y sistemas para detectar cualquier señal de actividad anómala tras la restauración del sistema.

- **Revisión y mejora de políticas de seguridad**: Reforzar las políticas de seguridad y la gestión de parches para prevenir futuros incidentes. Asegúrese de que los sistemas estén configurados correctamente para recibir actualizaciones automáticas de seguridad.
    - Implementar un proceso de gestión de vulnerabilidades que priorice la identificación y corrección rápida de fallos de seguridad.

Conclusiones

La vulnerabilidad Dirty Frag en el kernel de Linux representa una amenaza crítica debido a su capacidad para permitir a los atacantes locales escalar privilegios y obtener acceso completo al sistema. Sin parche oficial disponible, esta vulnerabilidad debe ser tratada como una prioridad máxima para evitar la explotación en entornos de producción.

Las organizaciones del sector salud que utilicen sistemas basados en Linux corren el riesgo de comprometer la confidencialidad, integridad y disponibilidad de los datos sensibles de los pacientes y las operaciones críticas, especialmente en los Sistemas de Información Hospitalaria (SIH). La explotación de esta vulnerabilidad podría tener consecuencias graves para la prestación de servicios médicos y la protección de datos.

La aplicación inmediata de parches de seguridad es la medida más efectiva para mitigar el riesgo. Mientras tanto, deshabilitar módulos vulnerables y auditar los sistemas son pasos cruciales para contener la amenaza. Además, el fortalecimiento de las políticas de seguridad y

el uso de principios de mínimos privilegios son fundamentales para reducir la exposición a futuros ataques.

En caso de que el sistema sea comprometido, es esencial actuar de inmediato para aislar el sistema afectado, realizar un análisis forense para identificar la extensión del ataque y eliminar cualquier malware o herramientas de persistencia instaladas por los atacantes. La restauración desde copias de seguridad confiables y la actualización del kernel son pasos clave para erradicar la amenaza.

Después de abordar el incidente, las organizaciones deben realizar auditorías de seguridad periódicas, mejorar las políticas de gestión de parches y capacitar a su personal en seguridad informática. La implementación de medidas de seguridad más robustas y la autenticación multifactor ayudarán a prevenir futuros compromisos y protegerán los sistemas sensibles.

Fuentes:

TechRadar – *Dirty Frag: Major security flaw in Linux kernel exposes systems to root access*

Enlace: https://www.techradar.com/pro/security/another-major-linux-security-flaw-revealed-dirty-frag-allows-root-on-all-major-distros-with-no-patch-or-fix-available-yet

Descripción: Este artículo describe la vulnerabilidad Dirty Frag y sus implicaciones, incluyendo la exposición al acceso root en sistemas Linux.

OpenCVE – *Vulnerabilities Published (May 10, 2026)*

Enlace: https://app.opencve.io/?utm_source=chatgpt.com

Descripción: Base de datos de vulnerabilidades reportadas recientemente, incluye detalles sobre el impacto y las acciones correctivas a seguir para vulnerabilidades críticas.

CVEFeed – *CVE Vulnerability Feed*

Enlace: https://cvefeed.io/vuln/latest/?utm_source=chatgpt.com

Descripción: Plataforma que proporciona información detallada sobre vulnerabilidades en productos, incluyendo las asociadas con sistemas operativos Linux y sus parches.

Lynis – *Security Auditing Tool for Linux*

Enlace: https://cisofy.com/lynis/

Descripción: Herramienta de auditoría de seguridad que ayuda a identificar vulnerabilidades de seguridad en sistemas Linux y UNIX, recomendada para evaluar el estado de seguridad después de un incidente.

Rkhunter – *Rootkit Hunter*

Enlace: https://sourceforge.net/projects/rkhunter/

Descripción: Herramienta de detección de rootkits para sistemas Linux, útil para encontrar y eliminar amenazas persistentes en sistemas comprometidos.

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.