Alerta Vulnerabilidad
Fallo crítico de seguridad en Mozilla Firefox y Thunderbird

CSIRTSALUD-AV-20260520-48 **TLP: CLEAR**

Alerta ID:	048
Fecha del reporte:	20/05/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Fallo crítico de seguridad en Mozilla Firefox y Thunderbird
Herramienta de detección	N/A
Activo involucrado:	Mozilla Firefox y Thunderbird
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la identificación de nuevas vulnerabilidades críticas en **Mozilla Firefox y Thunderbird**, registradas como **CVE-2026-8973** y **CVE-2026-8974**, que afectan la gestión de memoria de estos productos. Estas fallas podrían permitir la ejecución de código arbitrario, lo que podría resultar en acceso no autorizado a estaciones de trabajo, comprometiendo la confidencialidad, integridad y disponibilidad de la información clínica y administrativa, 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 versiones afectadas de **Firefox o Thunderbird**, 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, estaciones

de usuario con acceso a portales clínicos, correo institucional, sistemas de registro de pacientes y otros componentes relacionados con la gestión de información crítica en salud.

Descripción:

Mozilla ha lanzado actualizaciones de seguridad para corregir vulnerabilidades críticas en **Firefox y Thunderbird**, identificadas como **CVE-2026-8973** y **CVE-2026-8974**. Estas fallas afectan la gestión de memoria de los productos, específicamente en la forma en que los navegadores y clientes de correo procesan ciertos objetos internos y estructuras de datos. Los atacantes podrían aprovechar estas vulnerabilidades para ejecutar código arbitrario en las estaciones de trabajo de los usuarios, permitiéndoles acceder de forma no autorizada a información sensible o comprometer la integridad de los sistemas utilizados en entornos de salud.

El fallo se encuentra en la **gestión de memoria y procesamiento de entradas complejas**, lo que significa que un atacante podría diseñar contenido malicioso (páginas web, correos electrónicos o archivos abiertos en los clientes afectados) para desencadenar la ejecución de código sin necesidad de permisos administrativos previos. Esta vulnerabilidad es particularmente crítica debido a su impacto potencial, ya que permitiría a los atacantes comprometer estaciones de trabajo que gestionan datos clínicos, administrativos o de pacientes, afectando la confidencialidad, integridad y disponibilidad de la información.

Las actualizaciones lanzadas por Mozilla abordan estas fallas reforzando la **seguridad en la gestión de memoria y procesamiento de datos**, eliminando los vectores que podrían permitir la ejecución de código arbitrario. La recomendación es aplicar las actualizaciones inmediatamente para mitigar el riesgo de explotación, ya que la vulnerabilidad ha sido

clasificada como de alto riesgo y su explotación podría tener consecuencias graves para la seguridad y privacidad de la información en el sector salud.

Consecuencias de la explotación

La explotación exitosa de las vulnerabilidades **CVE-2026-8973 y CVE-2026-8974** en Firefox y Thunderbird puede tener graves consecuencias tanto a nivel técnico como operativo para las organizaciones del sector salud. Entre las principales consecuencias se destacan las siguientes:

1. **Acceso no autorizado a estaciones de trabajo:** Los atacantes que aprovechen estas vulnerabilidades podrían ejecutar código arbitrario en las estaciones afectadas, permitiéndoles acceder a información sensible, manipular aplicaciones clínicas o administrativas y comprometer datos críticos de los sistemas de salud.
2. **Escalamiento de privilegios local**: Una vez explotadas las fallas de memoria, los atacantes podrían ejecutar código con los privilegios del usuario activo, y en algunos escenarios, utilizar vectores adicionales para escalar privilegios dentro del equipo o de la red interna.
3. **Manipulación o exfiltración de información sensible**: Con acceso a estaciones de trabajo comprometidas, los atacantes podrían modificar, eliminar o robar datos confidenciales, incluyendo información clínica de pacientes, datos administrativos o

credenciales de acceso, lo que representa un riesgo directo para la privacidad y seguridad de los datos.

4. **Compromiso de la infraestructura TI**: La explotación podría permitir movimientos laterales hacia otros sistemas interconectados en la infraestructura de salud, incluyendo servidores de correo, portales de gestión clínica, bases de datos o redes internas críticas.
5. **Riesgos reputacionales**: El compromiso de datos sensibles o la interrupción de servicios esenciales podría afectar la confianza de pacientes, socios, proveedores y reguladores, dañando la reputación de la organización de salud.
6. **Impacto regulatorio**: Las entidades que gestionan información personal de pacientes podrían enfrentar sanciones bajo normativas de protección de datos, como la Ley 1581 de 2012 en Colombia, la GDPR en Europa u otras regulaciones locales, debido a la exposición de datos sensibles sin las medidas de seguridad apropiadas

Modo de explotación del ataque

La explotación de las vulnerabilidades **CVE-2026-8973 y CVE-2026-8974** en **Firefox y Thunderbird** puede llevarse a cabo mediante las siguientes fases claramente definidas:

Fase 1 – Identificación de versiones vulnerables y creación de contenido malicioso

El ataque comienza cuando el atacante identifica estaciones de trabajo o usuarios que utilizan versiones vulnerables de Firefox o Thunderbird. A continuación, el atacante diseña contenido

especialmente manipulado, como páginas web, correos electrónicos o archivos adjuntos, que explotan fallas de memoria y estructuras internas del navegador o cliente de correo.

Fase 2 – Ejecución de código arbitrario en la estación de trabajo

Al procesar el contenido malicioso, la falla de memoria permite al atacante ejecutar código arbitrario en el contexto del usuario que ejecuta la aplicación afectada. Esto proporciona control parcial sobre la estación de trabajo, permitiendo acciones no autorizadas sobre archivos, credenciales o aplicaciones locales.

Fase 3 – Acceso a información sensible y manipulación de datos

Con el código ejecutándose en la estación de trabajo comprometida, el atacante puede acceder a información sensible, incluyendo datos clínicos, administrativos o credenciales de sistemas internos. Asimismo, puede manipular o exfiltrar datos, afectando la confidencialidad e integridad de la información de la organización de salud.

Fase 4 – Persistencia y evasión de detección

El atacante podría intentar mantener acceso persistente en la estación de trabajo afectada mediante técnicas de inyección de código en memoria, modificación de configuraciones locales o explotación de otros vectores disponibles. Al eludir soluciones de seguridad y antivirus, puede operar de manera encubierta durante períodos prolongados, aumentando el riesgo para la infraestructura de TI del sector salud.

Vulnerabilidades asociadas

- Las vulnerabilidades **CVE-2026-8973 y CVE-2026-8974** en Firefox y Thunderbird no dependen de la explotación de un fallo externo en otro software, sino que se originan

en **debolezas inherentes en la gestión de memoria y procesamiento de entradas complejas** de estos productos. Sin embargo, su explotación puede aprovechar las siguientes características mal gestionadas:

- **Fallas en la gestión de memoria:** La vulnerabilidad se debe a defectos en la administración de memoria de Firefox y Thunderbird, lo que permite que un atacante provoque corrupción de memoria y ejecute código arbitrario. Esta falla compromete la integridad del entorno del usuario, permitiendo que los atacantes actúen sobre la estación de trabajo sin autorización.
- **Procesamiento inseguro de contenidos complejos:** Las aplicaciones afectadas no validan correctamente objetos internos o estructuras de datos complejas provenientes de páginas web, correos electrónicos o archivos adjuntos. La falta de validación adecuada aumenta el riesgo de explotación, permitiendo que los atacantes ejecuten acciones maliciosas en la estación de trabajo del usuario.
- **Exposición de información sensible:** Si los atacantes logran ejecutar código arbitrario, podrían acceder a datos clínicos, administrativos o credenciales almacenadas en la estación de trabajo, aumentando el riesgo de exfiltración de información sensible del sector salud.
- **Falta de controles de seguridad adicionales:** La ausencia de mecanismos complementarios de protección, como perfiles de usuario restringidos, políticas de ejecución de código y sandboxing reforzado, agrava la vulnerabilidad. Esto permite que un atacante que explote estas fallas pueda operar con un impacto significativo en la confidencialidad e integridad de los datos.

Recomendaciones de detección y mitigación

Los equipos de seguridad, infraestructura y administración de TI en las organizaciones del sector salud deben priorizar la actualización inmediata de todas las estaciones de trabajo y clientes afectados hacia las versiones corregidas de **Firefox 151**, **Firefox ESR 140.11**, **Thunderbird 151** y **Thunderbird ESR 140.11**. Se recomienda verificar todos los equipos de escritorio, portátiles, terminales de usuarios clínicos y administrativos, así como entornos de prueba y contingencia, para asegurar que no permanezcan instancias desactualizadas que puedan ser explotadas.

Adicionalmente, se recomienda realizar un inventario técnico de todas las aplicaciones que dependen de navegadores Firefox y clientes Thunderbird para acceder a portales web clínicos, correos electrónicos institucionales o sistemas de gestión administrativa. Este inventario debe incluir versiones instaladas, perfiles de usuario y extensiones activas que puedan interactuar con la memoria y procesamiento de datos internos de la aplicación.

Entre las medidas prioritarias se recomienda aplicar las siguientes:

1. **Actualizar de forma prioritaria todos los navegadores y clientes de correo afectados** en estaciones Windows, Linux y macOS, garantizando que los usuarios accedan

únicamente a versiones parcheadas y evitando la coexistencia de versiones vulnerables.

2. **Fortalecer las políticas de ejecución de código y sandboxing** en los navegadores y clientes de correo, limitando la capacidad de ejecución de scripts o procesos externos desde contenidos web o correos no confiables.
3. **Revisar el ciclo de vida y manejo de extensiones y complementos**, dado que complementos mal configurados pueden amplificar la exposición de memoria y servir de vector para la explotación de la vulnerabilidad.
4. **Evitar el uso de versiones beta o no soportadas** en entornos de producción, ya que estas pueden carecer de parches de seguridad críticos para la gestión de memoria y procesamiento de entradas complejas.
5. **Fortalecer la instrumentación y registro de eventos** en los sistemas de endpoints:
    1. Monitorear bloqueos de memoria inesperados, errores de ejecución o cierres abruptos del navegador/cliente de correo.
    2. Registrar accesos a portales críticos desde estaciones vulnerables.
    3. Alertar sobre patrones anómalos de uso o ejecución de scripts dentro del contexto de la aplicación.
6. **Revisar configuraciones de seguridad de contenidos y correo**, incluyendo la validación de certificados, deshabilitación de ejecución automática de scripts y apertura

de archivos adjuntos en entornos aislados, para reducir la superficie de ataque y prevenir explotación remota de la memoria.

7. **Validar despliegues corporativos y entornos distribuidos**: si los navegadores o clientes de correo se usan con perfiles sincronizados, políticas de grupo o MDM, asegurar que las actualizaciones y configuraciones de seguridad se aplican de forma consistente en todas las estaciones, evitando que un usuario quede con una versión vulnerable expuesta a la explotación

Recomendaciones de prevención y mitigación

Para prevenir la explotación de las vulnerabilidades **CVE-2026-8973 y CVE-2026-8974** y fortalecer la seguridad de las estaciones de trabajo y clientes de correo en el sector salud, se recomienda implementar las siguientes medidas de prevención y fortalecimiento:

1. **Aplicar las actualizaciones de seguridad de inmediato:** Las versiones parcheadas **Firefox 151**, **Firefox ESR 140.11**, **Thunderbird 151** y **Thunderbird ESR 140.11** deben ser instaladas en todos los equipos afectados, incluyendo estaciones de escritorio, portátiles y terminales de usuarios clínicos y administrativos. Asegúrese de que todas las estaciones tengan los navegadores y clientes de correo actualizados a las últimas versiones disponibles.
2. **Fortalecer la protección de ejecución de scripts y contenidos web/correo:** Active atributos de seguridad y restricciones para la ejecución de scripts en navegadores y

clientes de correo, incluyendo aislamiento de procesos, deshabilitación de ejecución automática de macros o scripts en adjuntos, y validación estricta de contenido HTML y JavaScript.

3. **Implementar perfiles de usuario restringidos y control de privilegios locales:** Limite los privilegios de los usuarios para reducir el impacto de la ejecución de código arbitrario. Incluso si un atacante explota la vulnerabilidad, la ejecución se limitará a un entorno controlado sin acceso administrativo al equipo o a la red interna.
4. **Revisar y controlar extensiones y complementos instalados:** Verifique que las extensiones de navegador o complementos de correo electrónico no introduzcan vectores adicionales de explotación, aplicando únicamente extensiones aprobadas y actualizadas según las políticas de seguridad corporativas.
5. **Rotación y revocación de perfiles de usuario en entornos críticos:** Si se sospecha que un equipo ha sido comprometido, restablezca perfiles y sesiones de usuario, limpiando cachés, cookies y datos temporales que podrían permitir persistencia de código malicioso.
6. **Monitoreo de eventos y registros de comportamiento anómalo:** Implementar un sistema de registro y alerta para detectar cierres inesperados del navegador, fallos de memoria, ejecuciones de scripts fuera de lo común, accesos a portales críticos o correos electrónicos con contenido malicioso. Configure alertas para detectar patrones sospechosos en estaciones de usuario.

7. **Evaluación periódica de vulnerabilidades en los clientes y estaciones:** Realice evaluaciones de seguridad automáticas y manuales en los navegadores y clientes de correo utilizados en la organización, identificando posibles vectores de explotación adicionales, configuraciones inseguras o versiones obsoletas.
8. **Defensa en profundidad:** Asegúrese de que los equipos cuenten con múltiples capas de seguridad, incluyendo firewall local, antivirus/EDR actualizado, control de tráfico de red, políticas de filtrado de contenido y restricciones de ejecución de scripts. Promueva buenas prácticas de seguridad informática entre los usuarios para prevenir futuras vulnerabilidades y minimizar riesgos operativos

Recomendaciones de respuesta ante compromiso

En caso de que se confirme un compromiso debido a la explotación de las vulnerabilidades **CVE-2026-8973 y CVE-2026-8974** en **Firefox y Thunderbird**, se deben seguir los siguientes pasos para contener el incidente, mitigar el daño y restaurar la seguridad de las estaciones de trabajo y sistemas afectados:

1. **Aislamiento de los sistemas comprometidos:** Desconectar inmediatamente las estaciones de trabajo afectadas de la red para evitar que la explotación se propague o que los atacantes mantengan el acceso no autorizado. Si el compromiso es masivo, considerar la desconexión temporal de todos los equipos que utilicen versiones vulnerables de Firefox o Thunderbird.

2. **Aplicación de actualizaciones de seguridad:** Instalar de forma urgente las versiones parcheadas de **Firefox 151**, **Firefox ESR 140.11**, **Thunderbird 151** y **Thunderbird ESR 140.11** en todos los sistemas afectados. Verificar que todas las estaciones de producción, pruebas y contingencia estén actualizadas.
3. **Revisión y limpieza de perfiles y sesiones:** Revocar perfiles de usuario, borrar cachés, cookies, credenciales y datos temporales que puedan haber sido manipulados durante la explotación. Asegurarse de que las sesiones de usuarios comprometidos sean reiniciadas y regeneradas en entornos seguros.
4. **Auditoría de registros y actividades:** Realizar una auditoría exhaustiva de los registros de eventos de las estaciones afectadas, incluyendo cierres inesperados de aplicaciones, errores de memoria, ejecución de scripts no autorizados y accesos a portales críticos. Monitorear patrones anómalos y acciones que puedan indicar explotación de la vulnerabilidad.
5. **Restablecimiento de credenciales y contraseñas:** Cambiar todas las contraseñas locales y de aplicaciones críticas que se usen en las estaciones comprometidas. Priorizar cuentas con privilegios elevados o acceso a información clínica y administrativa.
6. **Análisis forense de los equipos afectados:** Ejecutar análisis forense completo en las estaciones comprometidas para determinar el alcance del ataque, capturar logs y evidencias, y verificar la integridad de aplicaciones y configuraciones.

7. **Restauración desde copias seguras:** En caso de que se detecte manipulación de datos o instalación de software malicioso, restaurar los sistemas desde copias de seguridad verificadas y libres de vulnerabilidades. Confirmar que todas las restauraciones se realicen en entornos parcheados y seguros.
8. **Notificación y reporte interno:** Informar del incidente a los equipos de seguridad, CSIRT interno o responsable de TI. Si el compromiso involucra datos de pacientes, usuarios o información sensible, cumplir con las regulaciones de privacidad aplicables, como la **Ley 1581 de 2012** en Colombia o el **GDPR** en Europa.
9. **Comunicaciones con usuarios y pacientes:** Informar a los usuarios o responsables de los datos afectados sobre el incidente de manera clara y transparente, incluyendo las medidas adoptadas y los pasos recomendados para protegerse, como la actualización de software y cambios de credenciales.
10. **Revisión y fortalecimiento de medidas de seguridad:** Una vez mitigado el incidente, revisar la infraestructura de seguridad de los equipos y aplicaciones afectadas. Evaluar la implementación de políticas adicionales, como restricción de privilegios locales, sandboxing reforzado y, si es aplicable, autenticación multifactor (MFA) en portales internos críticos.

Conclusiones

Las vulnerabilidades **CVE-2026-8973 y CVE-2026-8974** representan un riesgo crítico para las estaciones de trabajo y clientes de correo utilizados en el sector salud. La explotación de estas fallas podría permitir la **ejecución de código arbitrario**, comprometiendo la **confidencialidad, integridad y disponibilidad** de la información clínica y administrativa.

El impacto de estas vulnerabilidades se extiende tanto a nivel técnico, afectando la seguridad de los endpoints y la integridad de los sistemas, como a nivel operativo, poniendo en riesgo la continuidad de procesos críticos de atención, gestión de datos de pacientes y operaciones administrativas.

La **aplicación inmediata de las actualizaciones de seguridad**, junto con la implementación de medidas de mitigación, monitoreo, auditoría y fortalecimiento de políticas de seguridad, es esencial para reducir el riesgo de explotación.

Además, es fundamental que las organizaciones del sector salud realicen **revisiones periódicas de sus estaciones de trabajo**, manteniendo los navegadores y clientes de correo actualizados, y aplicando buenas prácticas de seguridad para minimizar la exposición a vulnerabilidades futuras.

La adopción de estas acciones permitirá a las entidades de salud proteger la información sensible de pacientes, garantizar la continuidad de sus operaciones y cumplir con las regulaciones de privacidad vigentes, fortaleciendo así la seguridad integral de su infraestructura tecnológica.

Alerta Vulnerabilidad
Fallo crítico de seguridad en Mozilla Firefox y Thunderbird

CSIRTSALUD-AV-20260520-48 **TLP: CLEAR**

Fuentes:

- **Mozilla Security Advisories (MFSA 2026-46 y MFSA 2026-48)** – Publicaciones oficiales de Mozilla sobre vulnerabilidades de memoria en Firefox y Thunderbird.
  - MFSA 2026-46
  - MFSA 2026-48
- **National Vulnerability Database (NVD)** – Información técnica detallada sobre CVE-2026-8973 y CVE-2026-8974, incluyendo descripción, vector de ataque y calificación CVSS.
  - CVE-2026-8973
  - CVE-2026-8974
- **OpenCVE / CVEFeed** – Repositorios públicos que consolidan información sobre vulnerabilidades, versiones afectadas y parches disponibles.
  - CVE-2026-8973 y CVE-2026-8974 en OpenCVE
- **Boletines técnicos de actualización de Mozilla** – Documentación sobre versiones parcheadas, ESR y medidas de mitigación.
  - Firefox Release Notes 151
  - Thunderbird Release Notes 151

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.