Nro. Alerta:	AL-2025-004	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	24-ene-2025	**Vulnerabilidad en Mozilla Firefox y Mozilla Thunderbid**	Pág.: **1** of **4**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Información

Nivel de riesgo: Alto

II. ALERTA

Mozilla lanzó actualizaciones de seguridad para abordar vulnerabilidades en Firefox 134, con las que corrigen 11 vulnerabilidades, tres de estas son de alta gravedad. La más importante es la identificada con CVE-2025-0247 (CVSSv3 8.8) y está relacionada con un problema de corrupción de memoria que podría explotarse para ejecutar código arbitrario.

Figura 1.- *Ilustración asociada a FIrefox* ***Fuente: Linuxiac***

III. INTRODUCCIÓN

Los usuarios de Mozilla Firefox se enfrentan a una serie de vulnerabilidades de alta gravedad que podrían dejar los sistemas expuestos a ataques, destacando múltiples fallas de seguridad en el popular navegador y cliente de correo electrónico de Mozilla.

Estas vulnerabilidades de Mozilla, que afectan tanto a las versiones de escritorio como a las móviles, podrían provocar la ejecución de código arbitrario, la inestabilidad del sistema y la

escalada de privilegios. Mozilla ha publicado parches para solucionar estos problemas y se insta a los usuarios a actualizar su software de inmediato.

IV. VECTOR DE ATAQUE.

- **CVE-2025-0244:** es una vulnerabilidad de alto impacto en Firefox para Android que permite a los atacantes falsificar la barra de direcciones, lo que hace creer a los usuarios que están visitando un sitio web legítimo. Esta falla aumentó significativamente el riesgo de ataques de phishing y otras actividades maliciosas, lo que podría comprometer la seguridad del usuario.
- **CVE-2025-0245:** es una vulnerabilidad de impacto moderado en Firefox Focus para Android. Esta falla permite a los atacantes eludir la configuración de la pantalla de bloqueo, que está destinada a proteger la aplicación. Como resultado, personas no autorizadas podrían obtener acceso a la aplicación, lo que podría comprometer la privacidad y la seguridad del usuario.
- **CVE-2025-0246:** es una vulnerabilidad de alto impacto en Firefox para Android. Esta falla permite a un atacante falsificar la barra de direcciones. Este problema es diferente de CVE-2025-0244. Esta vulnerabilidad afecta a Firefox < 134.
- **CVE-2025-0237:** es una vulnerabilidad de impacto moderado en la API WebChannel, que se utiliza para la comunicación entre procesos tanto en Firefox como en Thunderbird. El problema surge porque la API WebChannel no logró validar correctamente el principio del remitente, lo que permitió a los atacantes aumentar sus privilegios y obtener acceso no autorizado al sistema afectado.
- **CVE-2025-0238:** esta vulnerabilidad afecta a Firefox < 134, Firefox ESR < 128.6, Firefox ESR < 115.19, Thunderbird < 134 y Thunderbird < 128.6. Suponiendo que se haya producido una asignación de memoria fallida y controlada, un atacante podría haber provocado un error de uso posterior a la liberación, lo que habría provocado un bloqueo potencialmente explotable
- **CVE-2025-0239:** es una vulnerabilidad de impacto moderado causada por un fallo en el manejo de la segmentación de texto de JavaScript. Este problema podría provocar daños en la memoria, lo que podría provocar fallos del sistema o permitir la ejecución remota de código, lo que comprometería la seguridad del sistema afectado.

- **CVE-2025-0240:** vulnerabilidad clasificada como crítica. Una función desconocida del componente JavaScript Module es afectada por esta vulnerabilidad. Mediante la manipulación de un input desconocido se causa una vulnerabilidad de clase desbordamiento de búfer. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad.
- **CVE-2025-0241:** esta vulnerabilidad afecta a Firefox < 134, Firefox ESR < 128.6, Thunderbird < 134 y Thunderbird < 128.6. Al segmentar texto especialmente diseñado, la segmentación corrompía la memoria y provocaba un bloqueo potencialmente explotable.
- **CVE-2025-0242:** destaca varios errores de seguridad de memoria encontrados tanto en Firefox como en Thunderbird, que suponen un alto riesgo de seguridad . Si se explotan, estas vulnerabilidades podrían permitir a atacantes remotos ejecutar código arbitrario, lo que podría comprometer la seguridad e integridad del sistema afectado.
- **CVE-2025-0243:** errores de seguridad de memoria presentes en Firefox 133, Thunderbird 133, Firefox ESR 128.5 y Thunderbird 128.5. Algunos de estos errores muestran evidencia de corrupción de memoria y puede aprovecharse para ejecutar código arbitrario.
- **CVE-2025-0247:** clasificado como crítica. Este problema afecta a una funcionalidad desconocida. La manipulación con una entrada desconocida provoca una vulnerabilidad de corrupción de memoria. El uso de CWE para declarar el problema provoca CWE-119. El producto realiza operaciones en un búfer de memoria, pero puede leer o escribir en una ubicación de memoria que está fuera del límite previsto del búfer. Se ven afectadas la confidencialidad, la integridad y la disponibilidad.

V. Impacto

Las vulnerabilidades en los productos de Mozilla afectan a varias versiones de Firefox y Thunderbird, incluidas las versiones estándar y Extended Support Release (ESR). En concreto, afectan a las siguientes versiones:

- Versiones de Mozilla Firefox anteriores a la 134
- Versiones de Mozilla Firefox ESR anteriores a 128.6 y 115.19
- Versiones de Mozilla Thunderbird anteriores a la 134
- Versiones de Mozilla Thunderbird ESR anteriores a 128.6 y 115.19

Estas vulnerabilidades son críticas, ya que representan un riesgo grave tanto para los usuarios individuales como para las empresas que dependen del software de Mozilla para navegar y comunicarse a diario. Sin la aplicación de parches, los atacantes podrían aprovechar estas vulnerabilidades para obtener acceso no autorizado, ejecutar código arbitrario o causar interrupciones significativas del sistema.

VI. RECOMENDACIONES:

- Actualizar a las últimas versiones del navegador Mozilla y del Correo Mozilla Thunderbird, monitorear la actividad sospechosa y habilitar funciones de seguridad como la autenticación multifactor. La aplicación de parches y el seguimiento de las mejores prácticas pueden reducir la exposición a estos riesgos .

VII. DESCARGO DE RESPONSABILIDAD.

- La información en la presente alerta, se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS.

- https://access.redhat.com/security/cve/CVE-2025-0238
- https://www.suse.com/security/cve/CVE-2025-0238.html
- https://vuldb.com/es/?id.290674
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-01/#CVE-2025-0242
- https://nvd.nist.gov/vuln/detail/cve-2025-0243
- https://www.suse.com/security/cve/CVE-2025-0246.html