



## Vulnerabilidad Zero Day de Firefox bajo ataque: Actualiza tu navegador web de inmediato

Mozilla ha anunciado una grave vulnerabilidad de seguridad que afecta a Firefox y a la versión de Soporte Extendido (ESR), la cual está siendo activamente explotada en entornos reales.

La falla, identificada como [CVE-2024-9680](#) (con un puntaje CVSS de 9.8), ha sido descrita como un error de uso después de liberar («use-after-free») en el componente de la línea de tiempo de animación.

«Un atacante logró ejecutar código en el proceso de contenido al aprovechar un uso después de liberar en las líneas de tiempo de animación», [explicó Mozilla](#) en un comunicado emitido el miércoles.

«Hemos recibido informes de que esta vulnerabilidad está siendo explotada en escenarios reales».

El descubrimiento y reporte de esta vulnerabilidad se le atribuye al investigador de seguridad Damien Schaeffer, de la empresa eslovaca ESET.

Este problema ha sido corregido en las siguientes versiones del navegador:

- Firefox 131.0.2
- Firefox ESR 128.3.1
- Firefox ESR 115.16.1

Actualmente, no se ha dado a conocer cómo se está aprovechando esta vulnerabilidad en ataques reales, ni quiénes son los responsables detrás de ellos.

A pesar de ello, vulnerabilidades de ejecución remota de código como esta podrían ser utilizadas de diversas formas, ya sea como parte de un ataque tipo «*watering hole*» dirigido a sitios web específicos o a través de [campañas de descarga](#) «*drive-by*» que engañan a los



## Vulnerabilidad Zero Day de Firefox bajo ataque: Actualiza tu navegador web de inmediato

usuarios para que visiten sitios web falsos.

Se recomienda a los usuarios actualizar a la versión más reciente para protegerse de estas amenazas activas.