Vulnerabilidades en Mozilla Firefox, Firefox ESR y Thunderbird

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de la Agencia de Ciberseguridad Vasca como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de la Agencia de Ciberseguridad Vasca. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

1. Resumen ejecutivo

Mozilla ha emitido avisos de seguridad donde se tratan múltiples vulnerabilidades que afectan al navegador **Firefox 125 y Firefox ESR**.

En relación a **Firefox 125** destacan **7 vulnerabilidades de severidad alta** cuyos identificadores son CVE-2024-3852, CVE-2024-3853, CVE-2024-3854, CVE-2024-3855, CVE-2024-3856, CVE-2024-3857 y CVE-2024-3858. De estas vulnerabilidades, 3 afectan también a **Firefox ESR**, sus identificadores son CVE-2024-3852, CVE-2024-3854 y CVE-2024-3857.

Estas vulnerabilidades, en caso de ser explotadas, podrían permitir ejecución de código arbitrario e instalación de programas, modificar y cambiar datos o crear nuevas cuentas con privilegios, comprometiendo así la confidencialidad e integridad de los sistemas. De momento, no se tiene constancia que dichas vulnerabilidades se estén explotando.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera los fallos destacados. Por lo que, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

2. Recursos afectados

- Mozilla Firefox versiones anteriores a 125
- Mozilla Firefox ESR – versiones anteriores a 115.10

3. Análisis técnico

Los detalles de las vulnerabilidades tratadas en este aviso son los siguientes:

En la vulnerabilidad CVE-2024-3852, **de severidad alta**, GetBoundName podría devolver la versión incorrecta de un objeto en caso de aplicar optimizaciones JIT. Este CVE afecta a versiones inferiores de Firefox 125 y a versiones inferiores de Firefox ESR 115.10.

La vulnerabilidad CVE-2024-3853, **de severidad alta**, afecta a versiones inferiores de Firefox 125 y es una vulnerabilidad en la que un programa puede seguir usando un recurso de memoria después de que este haya sido liberado, lo que puede permitir una ejecución de código malicioso.

La vulnerabilidad CVE-2024-3854, **de severidad alta**, afecta a versiones inferiores de Firefox 125 y a versiones inferiores de Firefox ESR 115.10 y puede ocurrir que, en algunos patrones de código, el compilador Just inTime – JIT, encargado de optimizar el código, optimice incorrectamente las sentencias switch y genere código fuera de las áreas de memoria.

La siguiente vulnerabilidad CVE-2024-3855, **de severidad alta**, afecta a versiones inferiores de Firefox 125. En este caso, el compilador JIT optimizar de manera incorrecta las operaciones de manipulación de cadenas de caracteres – Msubstr, lo que puede permitir acceder a partes de la memoria que no deberían ser accesibles.

La vulnerabilidad CVE-2024-3856**, de severidad alta**, afecta a versiones inferiores de Firefox 125. La explotación de este CVE podría permitir que un programa intente acceder a la memoria liberada, y comprometer la seguridad del sistema.

La vulnerabilidad CVE-2024-3857, **de severidad alta**, afecta a versiones inferiores de Firefox 125 y a versiones inferiores de Firefox ESR 115.10. En esta vulnerabilidad el compilador JIT produce código que no maneja correctamente los argumentos de una función o método, lo que podría permitir acceder a áreas de memoria liberadas.

La vulnerabilidad CVE-2024-3858, **de severidad alta**, afecta a versiones inferiores de Firefox 125. Este CVE puede permitir modificar un objeto Javascript de manera que el compilador JIT podría bloquearse al intentar seguir las referencias rastrear los cambios en ese objeto.

4. Mitigación / Solución

Como es habitual, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Para solucionar los problemas mencionados, Mozilla recomienda instalar la versión más reciente de Firefox. Las instrucciones para actualizar el navegador se encuentran disponibles en el siguiente enlace.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2024-3852.
- CVE-2024-3853.
- CVE-2024-3854.
- CVE-2024-3855.
- CVE-2024-3856.
- CVE-2024-3857.
- CVE-2024-3858.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY