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, Firefox ERS** y al cliente de correo electrónico multiplataforma **Mozilla Thunderbird**.

Dentro de estas, destacan 1 de **severidad crítica** cuyo identificador es CVE-2024-2615 y 7 de **severidad alta** cuyos identificadores son CVE-2024-2614, CVE-2024-2608, CVE-2024-2607, CVE-2024-2606, CVE-2024-2605, CVE-2024-2616 y CVE-2024-0743 que, de ser explotadas, pueden resultar en condiciones de desbordamiento de búfer basado en el Heap y ejecución arbitraria de código, entre otros.

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 anterior a la versión 124.
- Firefox ESR anterior a la versión 115.9.
- Firefox Thunderbird anterior a la versión 115.9.0.

3. Análisis técnico

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

La vulnerabilidad CVE-2024-2615, **de severidad crítica**, afecta a Firefox 123. Está causada por errores de seguridad en la memoria presentes en Firefox 123. Algunos de estos errores muestran evidencias de corrupción en la memoria, y su explotación podría posibilitar la ejecución arbitraria de código. La vulnerabilidad afecta a versiones de Firefox anteriores a la 124.

La vulnerabilidad CVE-2024-2614 afecta a las versiones de Firefox anteriores a la versión 124, a versiones de Firefox ESR anteriores a la 115.9 y a versiones del cliente de correo Thunderbird anteriores a la versión 115.9. El error está causado por fallos de seguridad presentes en la memoria que han mostrado evidencias de corrupción. **Este hecho podría haber sido explotado** permitiendo la ejecución de código arbitrario.

La vulnerabilidad CVE-2024-2605 afecta a versiones de Firefox anteriores a la 124, versiones de Firefox ESR anteriores a la versión 115.9 y a versiones del cliente de correo Thunderbird anteriores a la versión 115.9. Se ha detectado la posibilidad de uso de Windows Error Reportes como vector de escape de sandbox mediante la ejecución de código arbitrario en el sistema. **Este problema afecta únicamente a los sistemas operativos Windows.**

A continuación, la vulnerabilidad CVE-2024-2606, afecta a versiones de Firefox anteriores a la versión 124. El paso de datos inválidos podría haber resultado en la creación de valores wasm inválidos, como enteros arbitrarios que se convierten en valores de puntero.

La siguiente vulnerabilidad publicada, CVE-2024-2607, afecta a versiones de Firefox anteriores a la versión 124, Firefox ESR en versiones anteriores a la 115.9 y al cliente de correo Thunderbird en versiones anteriores a la 115.9. Se ha observado sobreescritura de los registros de retorno, este hecho podría permitir la ejecución de código arbitrario por parte de un atacante. **Este problema solo afecta a la arquitectura Armv7-A**.

La vulnerabilidad CVE-2024-2608 afecta a versiones de Firefox anteriores a la versión 124, a versiones de Firefox ESR anteriores a la 115.9 y a versiones del cliente de correo Thunderbird anteriores a la versión 115.9. Se ha observado posible desbordamiento de enteros en las funciones *AppendEncodedAttributeValue(), ExtraSpaceNeededForAttrEncoding() y AppendEncodedCharacters()*, lo que podría conducir a una subasignación de buffer de salida que podría causar escritura fuera de límites.

La vulnerabilidad CVE-2024-2616 afecta a versiones de Firefox ESR anteriores a la versión 115.9 y a versiones de Thunderbird anteriores a la versión 115.9. El

origen de la vulnerabilidad radica en el intento de fortalecimiento contra la explotación del conjunto de librerías ICU, utilizadas en Java y C/C++. Se cambió el comportamiento para las condiciones de falta de memoria para que, en lugar de intentar continuar, se produzca un fallo.

Por último, la vulnerabilidad CVE-2024-0743 afecta a versiones de Firefox ESR anteriores a la versión 115.9 y a versiones del cliente de correo Thunderbird anteriores a la versión 115.9. La vulnerabilidad tiene su origen en un valor de retorno no verificado en el código de protocolo de enlace TLS, este hecho podría causar un bloqueo potencialmente explotable.

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.

En el caso de Mozilla Thunderbird, las pautas de actualización se pueden consultar en el siguiente enlace.

5. Referencias Adicionales

- Avisos de seguridad.
- CVE-2024-2615.
- CVE-2024-2605.
- CVE-2024-2606.
- CVE-2024-2607.
- CVE-2024-2608.
- CVE-2024-2614.
- CVE-2024-2616.
- CVE-2024-0743.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY