Vulnerabilidad en Mozilla Thunderbird

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

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 un nuevo aviso de seguridad donde se trata una vulnerabilidad que afectan al cliente de correo electrónico multiplataforma **Mozilla Thunderbird**. La vulnerabilidad está considerada con una **criticidad alta** y cuenta con el identificador el CVE-2024-1936. El error produce el filtrado de asuntos de correos electrónicos cifrados a otras conversaciones, ya que el cifrado PGP puede cambiar el asunto de un correo, si selecciona otro, mientras el primero se está descifrando.

Debido a la política de seguridad del fabricante, por el momento no se han proporcionada información detallada para esta vulnerabilidad, con el fin de evitar su explotación. Debido a esto, las especificaciones técnicas pueden mantenerse restringidas hasta que la mayoría de los usuarios apliquen las actualizaciones de seguridad proporcionadas por el fabricante.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera el fallo destacado. 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

- Firefox Thunderbird versiones inferiores a 115.8.1.

3. Análisis técnico

Los detalles de la vulnerabilidad tratada en este aviso son los siguientes:

CVE-2024-1936: el asunto cifrado de un mensaje de correo electrónico podría asignarse de forma incorrecta y permanente a otro mensaje de correo electrónico arbitrario en la caché local de Thunderbird. En consecuencia, al responder al mensaje de correo electrónico contaminado, el usuario podría filtrar accidentalmente el asunto confidencial a un tercero.

4. Mitigación / Solución

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

Aunque esta actualización corrige el error y evita futuras contaminaciones de mensajes, no repara automáticamente las contaminaciones existentes. Se recomienda a los usuarios que utilicen la función de reparación de carpetas, disponible en el menú contextual de las carpetas de correo electrónico, que borrará las asignaciones incorrectas de asuntos.

Las pautas de actualización se pueden consultar en el siguiente enlace.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2024-1936.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY