



# Vulnerabilidades en Firefox y Firefox ESR

BCSC-AVISOS

**TLP: CLEAR**

[www.ciberseguridad.eus](http://www.ciberseguridad.eus)



## TABLA DE CONTENIDO

---

Sobre el BCSC.....	3
1. Aviso de seguridad.....	4
2. Recursos afectados .....	5
3. Análisis técnico .....	6
4. Mitigación / Solución.....	7
5. Referencias Adicionales .....	8

## Cláusula de exención de responsabilidad

---

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC 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 BCSC 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 BCSC. 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.

## Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.



El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:



## 1. Aviso de seguridad

---

Mozilla Foundation ha publicado dos [avisos de seguridad](#) donde corrige fallos para [Firefox](#) y [Firefox ERS](#), la versión del navegador Firefox para las grandes corporaciones, universidades y empresas. La severidad de ambos reportes está calificada como alta por el fabricante, en donde las vulnerabilidades más relevantes tratadas son [CVE-2022-46871](#), [CVE-2023-23598](#), [CVE-2023-23605](#), [CVE-2023-23597](#), [CVE-2023-23606](#), que cuentan con una severidad alta y para las que está disponible una actualización de seguridad para su mitigación.

## 2. Recursos afectados

---

- Firefox ESR 102.7
- Firefox 109

### 3. Análisis técnico

---

Los detalles de las vulnerabilidades más relevantes tratadas en esta actualización son los siguientes:

[CVE-2022-46871](#): vulnerabilidad que afecta a la biblioteca libusrctp que contenía fallos que podrían explotarse.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.8

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

- **Vector de ataque: Red**
- **Complejidad del ataque: Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario: Requerida**
- **Alcance: Sin cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

[CVE-2023-23598](#): vulnerabilidad que afecta al uso del código GTK de Firefox de texto plano para arrastrar datos, de forma que GTK trata todos los MIME de texto plano, que contienen URL de archivos, como si fueran arrastrados pudiendo conducir a que un sitio web pueda leer arbitrariamente un archivo a través de una llamada a `DataTransfer.setData`.

[CVE-2023-23605](#): errores de seguridad de memoria presentes en Firefox 108 y Firefox ESR 102.6. Algunos de estos errores mostraron evidencia de corrupción de memoria y podrían haber sido explotados para ejecutar código arbitrario.

[CVE-2023-23597](#): vulnerabilidad en donde un proceso secundario web comprometido podría deshabilitar las restricciones de apertura de la seguridad web, lo que provocaría la generación de un nuevo proceso secundario dentro del contexto `file://`. Este nuevo proceso podría explotarse de nuevo, lo que daría lugar a una lectura de archivos arbitraria.

[CVE-2023-23606](#): errores de seguridad de memoria presentes en Firefox 108 y Firefox ESR 102.6. Algunos de estos errores mostraron evidencia de corrupción de memoria y podrían haber sido explotados para ejecutar código arbitrario.

## 4. Mitigación / Solución

---

Para la mitigación de estas vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

En este caso el proveedor ya ha proporcionado una actualización para corregir los fallos reportados.

## 5. Referencias Adicionales

---

- [Mozilla Foundation](#)
- [Avisos de seguridad](#)
- [Firefox ERS](#)
- [CVE-2022-46871](#)
- [CVE-2023-23598](#)
- [CVE-2023-23605](#)
- [CVE-2023-23597](#)
- [CVE-2023-23606](#)



 Basque  
CyberSecurity  
Centre