Basque CyberSecurity Centre

Vulnerabilidades en Google Chrome

BCSC-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

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:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Aviso de seguridad

Google ha hecho público un aviso de seguridad donde se trata la actualización de Google Chrome a la versión 114, dentro del canal estable, que se encuentra disponible para su descarga y uso general. En el aviso se han resuelto un total de 16 errores, teniendo 8 una severidad calificada como alta por parte de la compañía y cuyos identificadores son CVE-2023-2929, CVE-2023-2930, CVE-2023-2931, CVE-2023-2932, CVE-2023-2933, CVE-2023-2934, CVE-2023-2935, CVE-2023-2936.

Debido a la política de seguridad de Google, por el momento no se han proporcionado detalles sobre estas vulnerabilidades, 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 Google.

2. Recursos afectados

- Google Chrome en versiones anteriores a la 114.0.5735.90 para Linux y Mac.
- Google Chrome en versiones anteriores a la 114.0.5735.90/91 para Windows.

3. Análisis técnico

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

CVE-2023-2929: vulnerabilidad de escritura fuera de los límites en Swiftshader que podría permitir a un atacante remoto explotar potencialmente la corrupción del heap a través de una página HTML manipulada.

CVE-2023-2930: vulnerabilidad Use-after-free en extensiones en Google Chrome en versiones anteriores a la 114.0.5735.90 que permite a un atacante, que engañe a un usuario, de instalar una extensión maliciosa para explotar potencialmente la corrupción del heap a través de una página HTML manipulada

CVE-2023-2931: vulnerabilidad Use-after-free en PDF en Google Chrome en versiones anteriores a la 114.0.5735.90 que permite a un atacante remoto explotar potencialmente la corrupción del heap a través de un archivo PDF manipulado.

CVE-2023-2932: vulnerabilidad Use-after-free en PDF en Google Chrome en versiones anteriores a la 114.0.5735.90 que permite a un atacante remoto explotar potencialmente la corrupción del heap a través de un archivo PDF manipulado.

CVE-2023-2933: vulnerabilidad Use-after-free en PDF en Google Chrome en versiones anteriores a la 114.0.5735.90 que permite a un atacante remoto explotar potencialmente la corrupción del heap a través de un archivo PDF manipulado.

CVE-2023-2934: vulnerabilidad de acceso a la memoria fuera de los límites en Mojo en Google Chrome en versiones anteriores a la 114.0.5735.90 que permite a un atacante remoto explotar potencialmente la corrupción del heap a través de una página HTML manipulada.

CVE-2023-2935: vulnerabilidad de confusión de tipos en V8 en Google Chrome anterior a 114.0.5735.90 que permite a un atacante remoto explotar potencialmente la corrupción del heap a través de una página HTML manipulada.

CVE-2023-2936: vulnerabilidad de confusión de tipos en V8 en Google Chrome anterior a 114.0.5735.90 que permite a un atacante remoto explotar potencialmente la corrupción del heap a través de una página HTML manipulada.

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.

Para ello, se deberá actualizar Google Chrome a la versión 114.0.5735.90 para Linux y Mac y a la versión 114.0.5735.90/91 para sistemas Windows. La solución oficial de seguridad puede descargarse de manera manual a través del siguiente enlace:

- Actualización de Google Chrome para Windows, Mac y Linux.

De manera adicional, Google ha proporcionado las instrucciones que destacan los pasos a seguir para poder actualizar el buscador Chrome de manera correcta, pudiendo acceder a dicha información mediante el siguiente enlace:

- Instrucciones para actualizar Google Chrome.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2023-2929.
- CVE-2023-2930.
- CVE-2023-2931.
- CVE-2023-2932.
- CVE-2023-2933.
- CVE-2023-2934.
- CVE-2023-2935.
- CVE-2023-2936.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA