Vulnerabilidades de severidad alta en Google Chrome

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

Google ha emitido un aviso de seguridad actualizando el canal estable 121.0.6167.160 para Mac y Linux y 121.0.6167.160/161 para Windows, que se lanzará en los próximos días/semanas, donde se corrigen **2 vulnerabilidades,** de **severidad alta** con los identificadores CVE-2024-1284 y CVE-2024-1283.

Debido a la política de seguridad de Google, por el momento no se han proporcionado información detallada para 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

- Canal estable en versiones anteriores a la 121.0.6167.160 para Mac.
- Canal estable en versiones anteriores a la 121.0.6167.160/161 en Linux y Windows.

3. Análisis técnico

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

CVE-2024-1284: vulnerabilidad Use-After-Free en Mojo.

CVE-2024-1283: vulnerabilidad de desbordamiento de búfer del Heap en Skia.

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 actualizar Google Chrome, la solución oficial de seguridad puede descargarse de manera manual a través del siguiente enlace:

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

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2024-1284.
- CVE-2024-1283.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY