Vulnerabilidades en Google Chrome

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

Google ha publicado un aviso de seguridad actualizando el canal de asistencia a largo plazo para **ChromeOS** en los sistemas **Windows, Mac y Linux**, donde se corrigen **3 vulnerabilidades** de **severidad alta** cuyos identificadores son CVE-2024-3157, CVE-2024-3516 y CVE-2024-3515.

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 de asistencia a largo plazo para Windows en versiones inferiores a 123.0.6312.122/.123.
- Canal de asistencia a largo plazo para Mac en versiones inferiores a 123.0.6312.122/.123/.124.
- Canal de asistencia a largo plazo para Linux en versiones inferiores a 123.0.6312.122.

3. Análisis técnico

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

CVE-2024-3157: vulnerabilidad de acceso a memoria fuera de los límites en el proceso de GPU Accelerated Compositing que permitía a un atacante remoto, que hubiese comprometido el proceso de GPU, realizar un escape de la sandbox mediante gestos de interfaz específicos. El fallo se produce en Google Chrome anterior a la versión 123.0.6312.122.

CVE-2024-3516: vulnerabilidad de desbordamiento de búfer de heap que afecta al proceso de la capa de abstracción ANGLE, que permitía a un atacante remoto explotar potencialmente la corrupción de heap a través de una página HTML manipulada. El fallo se produce en Google Chrome anterior a la versión 123.0.6312.122.

CVE-2024-3515: vulnerabilidad use after free en Dawn que permitía a un atacante remoto explotar potencialmente la corrupción de heap a través de una página HTML autogenerada. El fallo se produce en Google Chrome anterior a la versión 123.0.6312.122.

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 el canal LTS a la versión 123.0.6312.122/.123 en sistemas Windows, versión 123.0.6312.122/.123/.124 para sistemas Mac y versión 123.0.6312.122 en sistemas Linux. La solución oficial de seguridad para actualizar los canales de lanzamiento de Chrome se encuentra en el siguiente enlace.

Por último, 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-2024-3157.
- CVE-2024-3516.
- CVE-2024-3515.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY