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 avisos de seguridad donde, por una parte, se actualiza el canal LTS para **ChromeOS**, donde se corrigen **2 vulnerabilidades** de **severidad alta** cuyos identificadores son CVE-2024-0225 y CVE-2024-1059. Estas vulnerabilidades producen condiciones Use-After-Free en el software **WebGPU** y **WebRTC**.

Por otra, se actualiza el canal estable a la versión 122.0.6261.111/.112 para Windows y Mac, y 122.0.6261.111 para Linux, donde se corrigen **3 vulnerabilidades de severidad alta**, con los identificadores CVE-2024-2173, CVE-2024-2174 y CVE-2024-2176.

Adicionalmente, se incluyen soluciones de seguridad de terceros, entre los que se corrige el error CVE-2024-0646 en el kernel de Linux.

Debido a la política de seguridad de Google, no se ha proporcionado información detallada para algunas de 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 ChromeOS versión anteriores a LTS-114.0.5735.355 (plataforma: 15437.95.0).
- Google Chrome anterior a 121.0.6167.139.
- Canal estable versiones anteriores a la 122.0.6261.111/.112 para Windows y Mac.
- Canal estable versiones anteriores a la 122.0.6261.111 para Linux.

3. Análisis técnico

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

CVE-2024-0225: vulnerabilidad Use-After-Free en WebGPU en Google Chrome anterior a 120.0.6099.199 que permite a un atacante remoto explotar potencialmente la corrupción de Heap a través de una página HTML auto creada.

La métrica de evaluación de las vulnerabilidades se compone de:

CWE-416: Use After Free

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 de ataque: Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción del usuario:** Requerida
- **Ámbito de aplicación:** Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-1059: : vulnerabilidad Use-After-Free en Peer Connection en Google Chrome anterior a 121.0.6167.139 que permite a un atacante remoto explotar potencialmente la corrupción del Heap a través de una página HTML auto generada.

La métrica de evaluación de las vulnerabilidades se compone de:

CWE-416: Use After Free

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 de ataque: Baja**
- **Privilegios requeridos: Ninguno**
- **Interacción del usuario:** Requerida
- **Ámbito de aplicación:** Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-0646: vulnerabilidad de escritura de memoria fuera de límites en la funcionalidad de seguridad de la capa de transporte del kernel de Linux en cómo

un usuario llama a una función splice con un socket ktls como destino. Este fallo permite a un usuario local provocar un bloqueo o potencialmente escalar sus privilegios en el sistema.

La métrica de evaluación de las vulnerabilidades se compone de:

CWE 787: Out-of-bounds Write

CVSS Base: **7.8**

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

- **Vector de Ataque:** Local
- **Complejidad de ataque: Baja**
- **Privilegios requeridos: Bajos**
- **Interacción del usuario: Ninguna**
- **Ámbito de aplicación:** Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-2173: vulnerabilidad de acceso fuera de límites a la memoria en V8.

CVE-2024-2174: vulnerabilidad de implementación inapropiada en V8.

CVE-2024-2176: vulnerabilidad Use-After-Free en FedCM.

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 debe actualizar el canal estable para Windows, Mac y Linux. La solución oficial de seguridad para actualizar los canales de lanzamiento de Chrome se encuentra en el siguiente enlace.

Por últimos, se deberá actualizar el canal LTS a la versión 114.0.5735.355 (versión de plataforma: 15437.95.0). 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

- Avisos de seguridad.
- CVE-2024-0225.
- CVE-2024-1059.
- CVE-2024-0646.
- CVE-2024-2173.
- CVE-2024-2174.
- CVE-2024-2176.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY