Basque CyberSecurity Centre

Vulnerabilidades en Google Chrome y ChromeOS

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 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. Resumen ejecutivo

Google ha hecho públicos dos avisos de seguridad, anunciando una actualización del escritorio en canal estable para Google Chrome, y una actualización del canal de asistencia para ChromeOS.

El aviso en canal estable contiene un total de 10 vulnerabilidades, destacando una vulnerabilidad crítica y seis altas, que han sido registradas bajo los siguientes identificadores:

- CVE-2023-0941: vulnerabilidad de severidad crítica que afecta al componente *Prompts*.
- CVE-2023-0927: vulnerabilidad de criticidad alta que afecta a la API de *Web Payments*.
- CVE-2023-0928: vulnerabilidad de severidad alta que afecta al componente *SwifhShader*.
- CVE-2023-0929: vulnerabilidad de criticidad alta que afecta al componente *Vulkan*.
- CVE-2023-0930: vulnerabilidad de severidad alta que afecta al componente *Video*.
- CVE-2023-0931: vulnerabilidad de criticidad alta que afecta al componente *Video*.
- CVE-2023-0932: vulnerabilidad de severidad alta que afecta al componente *WebRTC*.

Del mismo modo, el aviso del canal de asistencia para ChormeOS, contiene un total de 5 errores, que han sido todos ellos calificados con una severidad alta y registrados bajo los siguientes identificadores:

- CVE-2023-0128: vulnerabilidad que afecta a *Overview Mode*.
- CVE-2023-0129: vulnerabilidad que afecta a *Network Services*.
- CVE-2022-4139: vulnerabilidad que afecta a *Linux Kernel*.
- CVE-2022-4378: vulnerabilidad que afecta a *Linux Kernel*.
- CVE-2022-45934: vulnerabilidad que afecta a *Linux Kernel*.

El fabricante ya ha publicado las actualizaciones correspondientes, corrigiendo de esta manera los fallos destacados. Por lo que, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

2. Análisis técnico

Una vez se han identificado las actualizaciones de seguridad propuestas por parte de Google, se deben destacar un total de 7 vulnerabilidades que afectan a Google Chrome y 5 que se dirigen contra ChromeOS.

Con respecto al aviso en el canal estable, el primer error que está identificado bajo el CVE-2023-0941 y que cuenta con una severidad crítica, es un fallo que existe debido a un error *use-after-free* en el componente *Prompts* de Google Chrome. Un atacante remoto puede crear una página web maliciosa, engañar a un usuario para que la visite, desencadenar el error mencionado y ejecutar código arbitrario en el sistema de destino.

En segunda instancia, la vulnerabilidad registrada como CVE-2023-0927, ha sido calificada con una criticidad alta. Dicho fallo es causado debido a un *use-after-free* en la API del componente *Web Payments* de Google Chrome. Un atacante remoto puede crear una página web maliciosa, engañar a la víctima para que la visite y ejecutar código arbitrario en el sistema de destino.

Seguidamente, el fallo catalogado bajo el CVE-2023-0928 y cuya severidad ha sido puntuada como alta, existe debido a un error *use-after-free* que se dirige contra el componente *SwiftShader*. Un atacante remoto puede crear una página web maliciosa, engañar a la víctima para que la visite, desencadenar el error destacado y ejecutar código arbitrario en el sistema vulnerable.

El cuarto error reportado conocido como CVE-2023-0929, ha sido calificado con una severidad alta por parte del fabricante. Dicha vulnerabilidad se debe a un error *use-after-free* en el componente *Vulkan*, que puede permitir a un atacante remoto crear una página fraudulenta, engañar a la víctima para que la visite, desencadenar el error descrito y ejecutar código arbitrario en el sistema de destino.

La quinta vulnerabilidad, registrada bajo el CVE-2023-0930, cuenta con una criticidad alta, asignada por parte del fabricante. Dicho error existe debido a un *boundary error* en el momento de procesar contenido HTML malicioso en el componente *Video*. Un atacante remoto puede crear una página web corrupta, engañar a la víctima para que la abra, desencadenar un desbordamiento de búfer y ejecutar código arbitrario en el sistema de destino.

El siguiente error, identificado como CVE-2023-0931 y que de igual manera tiene una puntuación alta, está causado por un error *use-after-free* en el componente *Video* de Google Chrome. Un atacante remoto puede crear una página web no fiable, engañar a la víctima para que la visite, desencadenar el error destacado y ejecutar código arbitrario en el sistema de destino.

En último lugar con respecto a las vulnerabilidades de Google Chrome, la vulnerabilidad registrada como CVE-2023-0932, que del mismo modo cuenta con una puntuación alta, existe debido a un error *use-after-free* en el componente *WebRTC* de Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite y ejecutar código arbitrario en el sistema de destino.

En relación a las vulnerabilidades que afectan a ChromeOS, el primer error destacado en el aviso está identificado bajo el CVE-2023-0128 y al igual que el resto de fallos, cuenta con una puntuación alta. Dicho fallo existe debido a un error *use-after-free* en el componente *Overview Mode*. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite y ejecutar código arbitrario en el sistema de destino.

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**

La segunda vulnerabilidad, registrada como CVE-2023-0129, se produce debido a *boundary error* al procesar contenido HTML no fiable en *Network Service*. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la abra, desencadenar un desbordamiento de búfer y ejecutar código arbitrario en el sistema de destino.

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**

Seguidamente, el fallo identificado bajo el CVE-2022-4139, existe debido a un *boundary error* dentro del controlador del *kernel i915* en el kernel Linux. Un usuario local puede provocar la corrupción de memoria y ejecutar código arbitrario con privilegios elevados.

La métrica de evaluación de la vulnerabilidad se compone de:

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 del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

En cuarto lugar, la vulnerabilidad que se le ha asignado el CVE-2022-4378, está provocada por un *boundary error* en la función *__do_proc_dointvec()*. Un usuario local puede provocar un desbordamiento de búfer y ejecutar código arbitrario con privilegios elevados.

La métrica de evaluación de la vulnerabilidad se compone de:

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 del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

Con respecto al último error destacado que afecta a ChromeOS, se encuentra el fallo registrado bajo el CVE-2022-45934. La vulnerabilidad existe por un desbordamiento de enteros dentro de la función *l2cap_config_req()* en en el kernel Linux. Un usuario local puede pasar paquetes *L2CAP_CONF_REQ* especialmente diseñados al dispositivo y ejecutar código arbitrario con privilegios elevados.

La métrica de evaluación de la vulnerabilidad se compone de:

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 del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

Finalmente, los productos afectados por las anteriores vulnerabilidades son los siguientes:

- Google Chrome versión 110.0.5481.104 y anteriores.
- ChromeOS versión 109.0.5414.94 y anteriores.

3. Mitigación / Solución

Como es habitual, para prevenir esta y otras 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 110.0.5481.177/.178 para Windows y a la versión 110.0.5481.177 para sistemas Mac y Linux. 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.

Con respecto a los sistemas ChromeOS, deberán ser actualizados a la versión 108.0.5359.221, siguiendo las instrucciones recalcadas en el siguiente enlace:

- Cómo actualizar el sistema operativo del Chromebook.

4. Referencias Adicionales

- Google Chrome.
- ChromeOS.
- Stable Channel Desktop Update.
- Long Term Support Channel Update for ChromeOS.
- CWE-416: Use After Free.
- CWE-122: Heap-based Buffer Overflow.
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer.
- CWE-190: Integer Overflow or Wraparound.
- Web Payments.
- SwiftShader.
- Boundary error.
- WebRTC.
- Network Service.
- Instrucciones para actualizar Google Chrome.
- Cómo actualizar el sistema operativo del Chromebook.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA