Basque CyberSecurity Centre

Vulnerabilidades en 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 público un aviso de seguridad, anunciando una actualización del canal de asistencia para ChromeOS. El aviso del canal de asistencia para ChormeOS, contiene un total de 3 errores, que han sido todos ellos calificados con una severidad alta y registrados con los identificadores CVE-2023-2135, CVE-2023-2134, CVE-2023-2133. La explotación de todos estos fallos supondría un impacto de alta gravedad en la disponibilidad, integridad y confidencialidad de los sistemas afectados.

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

2. Análisis técnico

Los detalles de las vulnerabilidades corregidas en esta actualización son:

CVE-2023-2134: vulnerabilidad de acceso a la memoria fuera de los límites en la API de Service Worker en Google Chrome antes de la versión 112.0.5615.137 que permite a un atacante remoto explotar potencialmente la corrupción del heap a través de una página HTML manipulada.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 787: Out-of-bounds Write

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**

CVE-2023-2133: vulnerabilidad de acceso a la memoria fuera de los límites en la API de Service Worker en Google Chrome antes de la versión 112.0.5615.137 que permite a un atacante remoto explotar potencialmente la corrupción del heap a través de una página HTML manipulada.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 787: Out-of-bounds Write

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**

CVE-2023-2135: vulnerabilidad Use-After-Free en DevTools en Google Chrome antes de la versión 112.0.5615.137 que permite a un atacante remoto, que

engañe a un usuario, a habilitar condiciones previas específicas y explotar potencialmente la corrupción del heap a través de una página HTML manipulada.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 416: Use After Free

CVSS Base: 7.5

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

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: Alta
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: Requerida
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

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

- Para la mayoría de los dispositivos ChromeOS, LTS-108 se está actualizando en el canal LTS a la versión 108.0.5359.231, para la versión de la plataforma 15183.94.0.

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.

Con respecto a los sistemas ChromeOS, deberán ser actualizados a la versión 108.0.5359.231, siguiendo las instrucciones recalcadas en el siguiente enlace:

- Cómo actualizar el sistema operativo del Chromebook.

4. Referencias Adicionales

- Actualización del canal de asistencia.
- CVE-2023-2135.
- CVE-2023-2134.
- CVE-2023-2133.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA