Basque CyberSecurity Centre

Vulnerabilidades en ChromeOS (CVE-2022-4437, CVE-2022-4436, CVE-2022-42720, CVE-2022-41674, CVE-2022-42719)

BCSC-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Sobre el BCSC 3
1. Aviso de seguridad 4
2. Recursos afectados 5
3. Análisis técnico 6
4. Mitigación / Solución 6
5. Referencias Adicionales 10

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 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 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. Aviso de seguridad

Google publicó el pasado 5 de enero de 2023, una nota de seguridad en donde se corrigen 5 fallos que afectan al sistema operativo ChromeOS y al navegador Google Chrome. Las vulnerabilidades, cuyos identificadores son, CVE-2022-4437, CVE-2022-4436, CVE-2022-42720, CVE-2022-41674, CVE-2022-42719 son de tipo use-after-free, fallos que se producen cuando un programa usa una dirección de memoria que previamente se ha liberado, y que puede producir consecuencias adversas que van desde la denegación de servicio, la ejecución de código arbitraria o la filtración de datos de la memoria.

2. Recursos afectados

- Mojo IPC
- Blink Media
- Kernel de Linux

3. Análisis técnico

El detalle de las vulnerabilidades tratadas es el siguiente:

CVE-2022-4437: vulnerabilidad use-after-free en Mojo IPC en Google Chrome en versiones anteriores a la 108.0.5359.124 de manera que se permite que un atacante remoto pueda explotar la corrupción del heap a través de una página HTML manipulada.

La métrica de evaluación de la vulnerabilidad es la siguiente:

CVSS Base: 8.8, alta

CWE 416: Use After Free

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-2022-4436: vulnerabilidad use-after-free en Blink Media en Google Chrome en versiones anteriores a la 108.0.5359.124 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 es la siguiente:

CVSS Base: 8.8, alta

CWE 416: Use After Free

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-2022-42720: Los atacantes, de forma local, que sean capaces de inyectar marcos WLAN, podrían usar varios errores de refcounting en el manejo de

múltiples BSS en la pila mac80211 en el Kernel de Linux versiones de la 5.1 a 5.19.x y anterior a la 5.19.16 para activar condiciones de use-after-free para ejecutar potencialmente código.

La métrica de evaluación de la vulnerabilidad es la siguiente:

CVSS Base: 7.8, alta

CWE 416: Use After Free

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**

CVE-2022-41674: vulnerabilidad que produce un problema en el kernel de Linux antes de la versión 5.19.16. Los atacantes capaces de inyectar tramas WLAN podrían provocar un desbordamiento del búfer en la función ieee80211_bss_info_update en net/mac80211/scan.c.

La métrica de evaluación de la vulnerabilidad es la siguiente:

CVSS Base: 8.8, alta

CWE 122: Desbordamiento de búfer basado en el heap

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

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

CVE-2022-42719: vulnerabilidad use-after-free que permite que los atacantes, capaces de inyectar marcos WLAN, puedan liberar en la pila mac80211, tras aplicar condiciones de use-after-free, el analizar un elemento multi-BSSID en el kernel de Linux 5.2 a 5.19.x antes de 5.19.16 para bloquear el Kernel y potencialmente ejecutar código.

La métrica de evaluación de la vulnerabilidad es la siguiente:

CVSS Base: 8.8, alta

CWE 416: Use After Free

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

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

4. Mitigación / Solución

Para la mitigación de estas vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Para solucionar estos fallos, desde Google se recomienda actualizar a las últimas versiones disponibles de cada herramienta.

5. Referencias Adicionales

- Notas de seguridad de Google
- use-after-free
- CVE-2022-4437
- CVE-2022-4436
- CVE-2022-42720
- CVE-2022-41674
- CVE-2022-42719
- CWE 416
- CWE 122
- ChromeOS


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA