OPENLINK

SISTEMAS DE REDES DE DATOS

Vulnerabilidad de Ejecución de Código Arbitrario en Google Chrome

Google Chrome es propenso a una vulnerabilidad de ejecución de código arbitrario.
Los atacantes pueden explotar este problema para ejecutar código arbitrario en el contexto del navegador, los intentos fallidos probablemente causarán una condición de denegación de servicio.
Las versiones de Google Chrome anteriores a 72.0.3626.121 son vulnerables.

Impacto de la vulnerabilidad	Severidad	CVE	Fecha de Publicación
Disponibilidad del servicio	Alta	CVE-2019-5786	01/03/2019

Información sobre el sistema/producto afectado

Las siguientes versiones de Chrome se ven afectadas:
De 72.0.3626.119 a la versión 72.0.3626.121

¿Cómo determinar si tenemos alguna de estas versiones afectadas?

Para determinar si es afectado por esta vulnerabilidad, es suficiente con verificar la versión:
1. Abre Google Chrome. Para abrirlo, haz doble clic sobre el acceso directo de Google Chrome que se encuentra en tu escritorio.
2. Haz clic en el botón de menú. Este botón abre el menú de opciones de Google Chrome. Lo puedes encontrar en la esquina superior derecha de la pantalla.
En versiones viejas, este botón tiene la forma de una llave inglesa y se encuentra en la parte derecha de la barra de direcciones.
En las últimas versiones, es un botón con rayas horizontales.

3. Desde el menú desplegable, selecciona “Configuración“. La página para configurar Google Chrome se abrirá en una pestaña nueva del navegador.
4. En la lista de opciones de la parte izquierda de la ventana, presiona “Ayuda“. Al hacerlo, llegarás a una página llamada “Información de Google Chrome“. Esta página contiene toda la información acerca de tu navegador, incluyendo la versión.
También puedes acceder directamente a la sección de ayuda seleccionando “Información de Google Chrome“ en lugar de “Configuración“ desde el menú desplegable.

¿Qué impacto tendría si la vulnerabilidad es explotada?

Causará una condición de denegación de servicio.

¿Qué hacer si tenemos la vulnerabilidad?

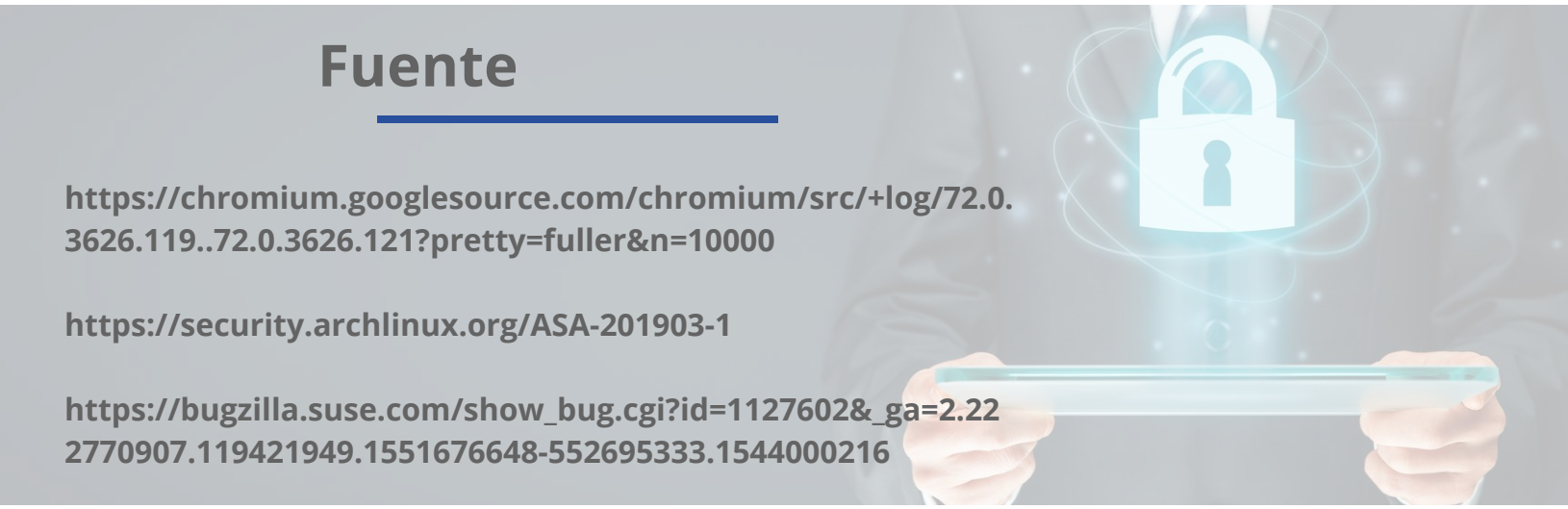
Las actualizaciones están disponibles. Por favor, consulte las referencias o asesoría del proveedor para obtener más información.
(https://chromereleases.googleblog.com/2019/03/stable-channel-update-for-desktop.html)

Fuente

https://chromium.googlesource.com/chromium/src/+log/72.0.3626.119..72.0.3626.121?pretty=fuller&n=10000

https://security.archlinux.org/ASA-201903-1

https://bugzilla.suse.com/show_bug.cgi?id=1127602&_ga=2.222770907.119421949.1551676648-552695333.1544000216



Sobre Nosotros

OPENLINK Sistemas de Redes de Datos, es una compañía regional con más de 20 años de experiencia en la entrega de soluciones y servicios, convirtiéndonos en el mejor aliado tecnológico para el cumplimiento de los objetivos de negocio de nuestros clientes.

Estamos activos en Colombia, Puerto Rico y Venezuela, con un equipo altamente calificado que nos permite expandirnos con éxito en Latinoamérica y el Caribe.

SI DETECTA ALGÚN EVENTO DE ESTE TIPO EN SU RED, NO DUDE EN PONERSE EN CONTACTO CON EL NOC/SOC DE OPENLINK:

soc@oplk.com
mercadeo@oplk.com
+58 212 273 4300 Op. 1-2
+57 1 432 1740 Ext. 574430
+1 787 273 0876