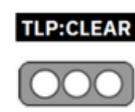


Nro. Alerta:	AL-2024-008	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	14-may-2024	Vulnerabilidad en Google Chrome	V 1.1 Pág.: 1 of 3

I. DATOS GENERALES:

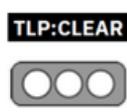
Clase de alerta:	Vulnerabilidad
Tipo de incidente:	Vulnerabilidad
Nivel de riesgo:	Alto

II. ALERTA

Google ha lanzado con urgencia otra actualización de seguridad para su popular navegador Chrome. Esta vez, la medida se ha tomado debido al descubrimiento de una vulnerabilidad crítica con explotación activa en ataques reales. La vulnerabilidad, identificada como CVE-2024-4671, representa un error de uso después de la liberación en el componente encargado de representar el contenido web. Esto significa que los atacantes pueden aprovechar esta vulnerabilidad para ejecutar código arbitrario en el contexto del navegador, lo que podría llevar a compromisos completos del sistema.



Figura 1.- CVE-2024-4671 – figura referencial

Nro. Alerta:	AL-2024-008	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	14-may-2024	Vulnerabilidad en Google Chrome	V 1.1 Pág.: 2 of 3

III. INTRODUCCIÓN

El hallazgo de esta peligrosa vulnerabilidad provino de un experto anónimo en ciberseguridad el 7 de mayo de 2024. Google respondió rápidamente a la advertencia y ha recomendado a los usuarios actualizar Chrome a las siguientes versiones:

- 24.0.6367.201/.202 para Windows y macOS, y
- 124.0.6367.201 para Linux.

La urgencia de esta actualización subraya la seriedad del problema y la importancia de proteger los sistemas contra posibles ataques.

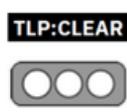
Google ha confirmado la existencia de un exploit para esta vulnerabilidad, aunque no ha proporcionado detalles sobre su uso en ataques ni información sobre los perpetradores detrás de ellos. Esta falta de información destaca la necesidad de una respuesta rápida por parte de los usuarios para protegerse contra cualquier posible explotación de esta vulnerabilidad.

IV. VECTOR DE ATAQUE:

CVE-2024-4671 (CVSS 8.8): Esta vulnerabilidad, catalogada como «uso después de la liberación», afecta al componente Visuals de Chrome, lo que implica un manejo incorrecto de la memoria dinámica durante la ejecución del programa. Si una aplicación no elimina correctamente un puntero de memoria después de liberarla, un atacante podría aprovechar esta situación para ejecutar código malicioso en el sistema, potencialmente obteniendo acceso no autorizado a datos sensibles o incluso control total sobre el sistema comprometido.

Versiones Afectadas:

- Versiones anteriores a la 124.0.6367.201/.202 para Mac y Windows.
- Versiones anteriores a la 124.0.6367.201 para Linux.

Nro. Alerta:	AL-2024-008	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	 ecucert
TLP:			
Fecha:	14-may-2024	Vulnerabilidad en Google Chrome	V 1.1 Pág.: 3 of 3

V. IMPACTO:

- Instalación de extensiones y software malicioso.
- Control total sobre el sistema comprometido
- Liberación de contraseñas.
- Fallas en la ejecución de códigos remotos.

VI. RECOMENDACIONES:

- Aplicar las actualizaciones de inmediato para protegerse contra la explotación de la vulnerabilidad.
- Aplicar futuras actualizaciones de seguridad tan pronto como estén disponibles para mantener una protección continua contra amenazas emergentes.

VII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS:

<https://osint.com.ar/google-lanza-una-actualizacion-urgente-para-chrome-tras-descubrir-una-vulnerabilidad-critica/>

<https://csirt.telconet.net/comunicacion/noticias-seguridad/nuevo-exploit-zero-day-afecta-a-google-chrome/>