Nro. Alerta:	AL-2025-058	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	7-nov-2025	Vulnerabilidades Críticas – Google Chrome	Pág.: **1** of **4**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad crítica en Chrome
Tipo de Incidente: Explotación de vulnerabilidades (RCE / Corrupción de memoria)
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Vulnerabilidades Críticas – Google Chrome - Figura referencial

Google ha lanzado una actualización de emergencia para su navegador Chrome con el fin de corregir múltiples vulnerabilidades de alto riesgo, entre las que se incluyen la ejecución remota de código (RCE) y corrupción de memoria. Entre ellas, destacan tres fallos específicos: CVE-2025-12725, que es un desbordamiento de búfer en WebGPU; CVE-2025-12726, una implementación inapropiada en los componentes de Views; y CVE-2025-12727, una implementación incorrecta en el motor V8.

III. INTRODUCCIÓN

Con esta nueva actualización Google parchea varias vulnerabilidades de alta gravedad que representan riesgos significativos para la seguridad del usuario, tales como:

CVE-2025-12725: Falla de escritura fuera de límites en WebGPU que permite corrupción de memoria y ejecución remota de código mediante contenido web malicioso. Afecta el renderizado de gráficos acelerados por GPU en aplicaciones web.
CVE-2025-12726: Implementación inapropiada en el componente Views que permite manipulación de la interfaz de usuario y ejecución de código remoto a través de páginas web diseñadas maliciosamente.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

CVE-2025-12727: Implementación inapropiada en V8, un Falla en el motor V8 de JavaScript que permite corrupción de memoria (heap) y ejecución de código remoto mediante scripts especialmente diseñados.

Las vulnerabilidades de ejecución remota de código (RCE) en componentes como WebGPU y V8 son especialmente críticas, ya que permitirían que un sitio web malicioso comprometa el sistema del usuario con solo visitar la página, sin necesidad de ninguna interacción adicional. También entre las fallas críticas se incluyen problemas de escritura fuera de límites, implementaciones inapropiadas que permiten corrupción de memoria.

IV. VECTOR DE ATAQUE

Google ha restringido los detalles técnicos del exploit para evitar que los atacantes lo aprovechen antes de que la mayoría de los usuarios hayan aplicado la actualización.

Las vulnerabilidades tienen un vector de ataque tipo RED y su nivel de severidad CVSS:3.1 es de consideración alta:

- CVE-2025-12725, puntuación 8.8
- CVE-2025-12726, puntuación 8.1
- CVE-2025-12727, puntuación 8.8

V. IMPACTO

Todas las versiones de Google Chrome y navegadores basados en Chromium anteriores a la rama 142.0.7444.134/135 (es decir, cualquier build cuya versión sea menor a 142.0.7444.134 en las plataformas Windows, macOS y Linux). Se presume impacto similar en otros proyectos/embebidos de Chromium que no apliquen el parche de forma independiente.

VI. INDICADORES DE COMPROMISO

- Cualquier sitio o contenido web diseñado o infectado que contenga código JavaScript o WebAssembly malicioso.
- Cualquier sitio web que contenga videos, animaciones CSS, gráficos en 3D (webGL), canvas en 2D, sitios con efectos visuales y uso de filtros en los que emplee el uso de webGPU.
- Google Chrome versión v137.0.7151.68/.69 o inferiores.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

VII. RECOMENDACIONES:

- Actualizar de inmediato Google Chrome en todas las plataformas disponibles (Windows, macOS, Linux y Android) a la versión 142.0.7444.134/135 o superior, la cual contiene los parches que corrigen las vulnerabilidades críticas identificadas.
- Garantizar la aplicación de actualizaciones automáticas o, en entornos empresariales, implementar políticas forzadas de actualización mediante herramientas de gestión centralizada, con el fin de asegurar que todos los equipos adopten las versiones corregidas en el menor tiempo posible.
- Restringir temporalmente el uso de WebGPU y de extensiones con alto nivel de privilegio o procedencia dudosa, hasta confirmar que todos los navegadores del entorno operan con las actualizaciones aplicadas. Se recomienda bloquear la instalación de extensiones no verificadas que puedan ejecutar o almacenar código malicioso.
- Supervisar la actividad del navegador y establecer alertas frente a comportamientos anómalos, como cierres repentinos, consumo inusual de memoria GPU o conexiones hacia dominios desconocidos que sean iniciadas por el proceso del navegador.
- Revisar las políticas de control de extensiones, privilegios y sandboxing. Asegurar que el navegador funcione con los permisos mínimos necesarios y que las cuentas de usuario no cuenten con derechos administrativos que faciliten la explotación o propagación de un ataque.

VIII. 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.

IX. REFERENCIAS:

THE CYBER EXPRESS (2025). Google Chrome 142 Fixes RCE Flaws. https://thecyberexpress.com/google-chrome-142-fixes-rce-flaws/

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

CSIRT TELCONET (2025). Actualización de seguridad crítica para Google Chrome corrige múltiples vulnerabilidades de ejecución remota de código. https://csirt.telconet.net/comunicacion/noticias-seguridad/actualizacion-de-seguridad-critica-para-google-chrome-corrige-multiples-vulnerabilidades-de-ejecucion-remota-de-codigo/

CVE (2025). CVE-2025-12725. https://www.cve.org/CVERecord?id=CVE-2025-12725

CVE (2025). CVE-2025-12726. https://www.cve.org/CVERecord?id=CVE-2025-12726

CVE (2025). CVE-2025-12727. https://www.cve.org/CVERecord?id=CVE-2025-12727

ECUCERT (2025). Vulnerabilidad Crítica — Motor de JavaScript V8 (Navegadores Chromium). https://www.ecucert.gob.ec/wp-content/uploads/2025/10/AI-2025-057-Vulnerabilidad-Critica-Motor-de-JavaScript-V8-Navegadores-Chromium.pdf

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec