Nro. Alerta:	AL-2025-038	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	31-jul-2025	Vulnerabilidad crítica en Google Chrome (CVE-2025-6558)	Pág.: **1** of **3**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de Incidente: Ejecución remota de código (RCE) y escape de sandbox

Nivel de riesgo: Alta

II. ALERTA

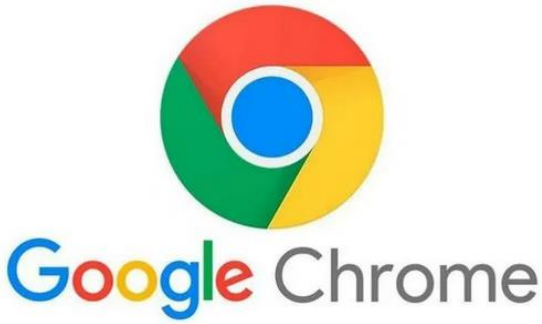

Figura 1. Vulnerabilidad crítica en Google Chrome (CVE-2025-6558) - Figura referencial

Se ha identificado la vulnerabilidad crítica en Google Chrome CVE-2025-6558, específicamente en los componentes ANGLE y GPU. Esta falla permite a atacantes remotos ejecutar código arbitrario mediante páginas HTML maliciosas, logrando evadir el sandbox (un entorno aislado de seguridad que protege a los usuarios de malware y amenazas) del navegador. La vulnerabilidad está siendo explotada activamente y ha sido incluida en el catálogo de vulnerabilidades explotadas conocidas (KEV) de CISA en julio de 2025.

III. INTRODUCCIÓN

La vulnerabilidad crítica en Google Chrome CVE-2025-6558, tiene una severidad alta (CVSS 8.8), permite a un atacante remoto evadir el entorno de seguridad (sandbox) del navegador al inducir a un usuario a visitar una página HTML maliciosa. Esta falla se encuentra en ANGLE (Almost Native Graphics Layer Engine), una biblioteca gráfica de código abierto que Chrome utiliza como intermediario para traducir instrucciones de OpenGL ES (versión simplificada del estándar OpenGL, OpenGL es la especificación estándar para una interfaz de programación de aplicaciones API multiplataforma y multilenguaje para renderizar gráficos 2D y 3D) hacia otras API gráficas como Direct3D (Windows), Metal (macOS), Vulkan u OpenGL

IV. VECTOR DE ATAQUE

El ataque se produce al inducir al usuario a visitar una página HTML maliciosa especialmente diseñada. ANGLE procesa comandos gráficos desde fuentes no confiables, como sitios que utilizan WebGL, por lo que los errores en este componente pueden permitir la ejecución de código arbitrario dentro del proceso de GPU del navegador, facilitando un posible escape del Sandbox. Aunque Google no ha publicado detalles técnicos completos, se confirma que esta explotación representa un alto riesgo de seguridad.

V. IMPACTO

Sistema Operativo	Versiones afectadas
Windows	Anteriores a 138.0.7204.157/.158
macOS	Anteriores a 138.0.7204.157/.158
Linux	Anteriores a 138.0.7204.157

Tabla 1.- Versiones Afectados - Vulnerabilidad crítica en Google Chrome (CVE-2025-6558)

VI. INDICADORES DE COMPROMISO

Actualmente, no se han publicado indicadores de compromiso específicos relacionados con esta vulnerabilidad. Sin embargo, se recomienda monitorear los sistemas en busca de actividades sospechosas, como la ejecución de procesos desconocidos o conexiones de red inusuales, especialmente después de que un usuario haya visitado una página web desconocida o sospechosa.

VII. RECOMENDACIONES:

- Asegúrese de que todos los sistemas utilicen la versión 138.0.7204.157 o superior de Google Chrome, donde esta vulnerabilidad ha sido corregida.
- Aplicar parches en sistemas operativos afectados: Apple ha lanzado actualizaciones críticas para iOS 18.6, iPadOS 18.6, macOS Sequoia 15.6 y otros sistemas operativos para abordar esta vulnerabilidad.
- Implemente soluciones de detección y respuesta (EDR) para identificar y responder a comportamientos anómalos que puedan indicar la explotación de esta vulnerabilidad.
- Eduque a los usuarios sobre los riesgos de hacer clic en enlaces desconocidos o descargar archivos de fuentes no confiables.
- Asegúrese de que las políticas de seguridad estén actualizadas y que se apliquen controles adecuados para prevenir la ejecución de código no autorizado.

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:

CSIRT TELCONET (2025). Google lanza actualización urgente por nueva vulnerabilidad crítica. https://csirt.telconet.net/comunicacion/boletines-servicios/google-lanza-actualizacion-urgente-por-nueva-vulnerabilidad-critica/

CYBERSECUREFOX (2025). Chrome: actualización crítica por vulnerabilidad CVE-2025-6558 explotada. https://cybersecurefox.com/es/chrome-actualizacion-critica-vulnerabilidad-cve-2025-6558-explotada/

SOC PRIME (2025). CVE-2025-6558 – Google Chrome Vulnerability. https://socprime.com/es/blog/cve-2025-6558-google-chrome-vulnerability/

NVD (2025). CVE-2025-6558 Detail. https://nvd.nist.gov/vuln/detail/CVE-2025-6558

BLEEPINGCOMPUTER (2025). Apple patches security flaw exploited in Chrome zero-day attacks. https://www.bleepingcomputer.com/news/security/apple-patches-security-flaw-exploited-in-chrome-zero-day-attacks/

CERT PARAGUAY (2025). Vulnerabilidades en Google Chrome. https://www.cert.gov.py/vulnerabilidades-en-google-chrome-8/