I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad crítica en Chrome
Tipo de Incidente: Múltiples vulnerabilidades en Google Chrome, incluida una vulnerabilidad Zero-Day en V8
Nivel de riesgo: Alta

II. ALERTA

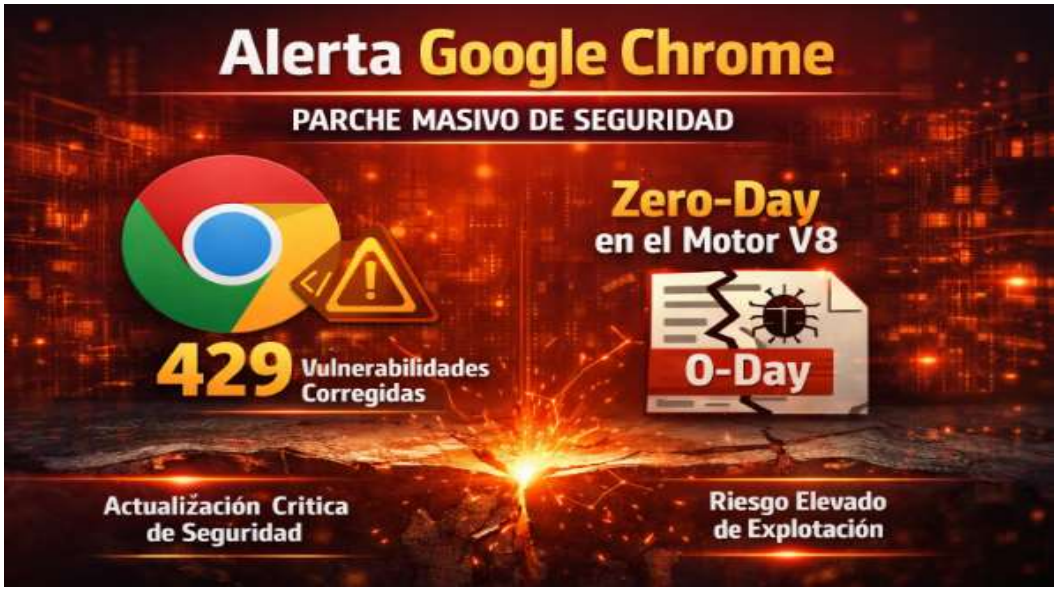

Figura 1.- Google Chrome (429 vulnerabilidades y zero-day en V8) - Figura referencial

Google liberó Chrome 149, una actualización de seguridad que corrige 429 vulnerabilidades, incluidas 22 fallas críticas identificadas desde CVE-2026-10881 hasta CVE-2026-10902, siendo principalmente la mayoría fallas de tipo use-after-free (uso tras liberación) UAF, detectada en componentes gráficos como ANGLE y WebGL, Posteriormente, se detectó una nueva vulnerabilidad zero-day denominada CVE-2026-11645 que estaba siendo explotada activamente y de tipo out-of-bounds read/write (lectura/escritura fuera de limites) en el motor V8. Estas fallas podrían provocar corrupción de memoria, ejecución remota de código o evasión del sandbox del navegador, permitiendo a un atacante ejecutar código arbitrario mediante una página HTML especialmente diseñada.

III. INTRODUCCIÓN

Chrome 149 es el nombre de la versión estable 149.0.7827.X, un paquete de actualización que Google libero para corregir 429 vulnerabilidades de seguridad compuestas

por 87 problemas de alto riesgo, 226 de riesgo medio, 94 de riesgo bajo y 22 fallas críticas.

Las fallas críticas están identificadas por los CVE-2026-10881 hasta CVE-2026-10902 y afectan componentes fundamentales del navegador, como el motor de JavaScript, los subsistemas gráficos y la interacción con la unidad de procesamiento gráfico (GPU). En su mayoría corresponden a vulnerabilidades de tipo use-after-free, que es una falla de corrupción de memoria que ocurre cuando un programa continúa utilizando un bloque de memoria después de haberlo liberado. Varias de estas vulnerabilidades afectan componentes gráficos como ANGLE y WebGL, lo que podría permitir a un atacante manipular el comportamiento del navegador o ejecutar código malicioso.

CVE-2026-11645 es una vulnerabilidad de tipo out-of-bounds read/write en V8, el motor de JavaScript y WebAssembly de Chrome. Esta falla podría permitir a un atacante remoto ejecutar código arbitrario dentro del entorno aislado (sandbox) del navegador mediante una página HTML especialmente diseñada. Google reconoció que existe un exploit de día cero (zero-day) para esta vulnerabilidad que estaba siendo explotada activamente.

IV. VECTOR DE ATAQUE

Se detalla el nivel de severidad de las 22 vulnerabilidades criticas:

CVE	Componente	Falla	Severidad
CVE-2026-10881	ANGLE	Lectura/Escritura fuera de límites	9.6
CVE-2026-10882	Network	Use-after-free	8.8
CVE-2026-10883	ANGLE	Escritura fuera de límites	8.8
CVE-2026-10884	Chromecast	Use-after-free	8.3
CVE-2026-10885	Chrome para iOS	Use-after-free	8.8
CVE-2026-10886	FileSystem	Use-after-free	9.6
CVE-2026-10887	Chromoting	Use-after-free	8.1
CVE-2026-10888	Cast Streaming	Use-after-free	8.8
CVE-2026-10889	ANGLE	Lectura fuera de límites	8.3
CVE-2026-10890	Cast	Use-after-free	8.8
CVE-2026-10891	GFX	Use-after-free	8.8
CVE-2026-10892	GPU	Escritura fuera de límites	9.6
CVE-2026-10893	Chromoting	Use-after-free	8.8
CVE-2026-10894	Printing	Use-after-free	8.3
CVE-2026-10895	Ozone	Use-after-free	8.8
CVE-2026-10896	Chrome para iOS	Use-after-free	8.8

CVE	Componente	Falla	Severidad
CVE-2026-10897	GPU	Escritura fuera de límites	8.8
CVE-2026-10898	GPU	Desbordamiento de buffer en pila	8.3
CVE-2026-10899	Ozone	Use-after-free	7.5
CVE-2026-10900	Password Manager	Use-after-free	7.5
CVE-2026-10901	Password Manager	Use-after-free	7.5
CVE-2026-10902	Ozone	Use-after-free	8.8
CVE-2026-11645	Motor V8	Lectura y escritura fuera de límites	8.8

Tabla 1.- Detalle de severidad de las diferentes vulnerabilidades - Google Chrome (429 vulnerabilidades y zero-day en V8

V. IMPACTO

Producto	Versiones afectadas	Plataformas / Sistemas Operativos	Componentes afectados
Google Chrome (Stable)	< 149.0.7827.102/.103	Windows, macOS, Linux	Navegador web
Google Chrome	Anteriores a 149.0.7827.x	Windows, macOS, Linux, Chrome para iOS y Chromecast	Motor V8, ANGLE, GPU, Network, Password Manager, WebRTC, WebView, DevTools y otros componentes del ecosistema Chrome

Tabla 2.-Versiones afectadas - Google Chrome (429 vulnerabilidades y zero-day en V8)

VI. INDICADORES DE COMPROMISO

Google informo que no se reportó explotación activa de las 22 vulnerabilidades críticas al momento del lanzamiento de la actualización, siendo la mayoría de las fallas descubiertas internamente por Google mediante una combinación de análisis manual y herramientas de seguridad asistidas por inteligencia artificial, mientras que otras fueron reportadas por investigadores externos a través de sus programas de recompensas (bug bounty), manteniendo la reserva de métodos e indicadores de compromiso.

Para CVE-2026-11645, Google confirmó la existencia de un exploit de zero-day, sin embargo, no ha revelado IoCs ni detalles adicionales, de acuerdo con sus políticas de seguridad y divulgación responsable.

VII. RECOMENDACIONES:

- Actualizar inmediatamente Google Chrome a la versión más reciente disponible en todos los sistemas afectados.

- Verificar que la actualización se haya instalado correctamente y que el navegador opere con normalidad después del proceso.
- Habilitar y mantener activas las actualizaciones automáticas para garantizar la aplicación oportuna de futuros parches de seguridad.
- Implementar la actualización de manera centralizada mediante las herramientas de gestión empresarial disponibles en la organización.
- Monitorear los registros de seguridad y la actividad de los equipos para detectar posibles intentos de explotación asociados a la vulnerabilidad zero-day en V8 y a los demás CVE corregidos.
- Restringir el uso de versiones obsoletas del navegador y promover la actualización inmediata de todos los usuarios.

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:

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

GOOGLE CHROME RELEASES. *https://chromereleases.googleblog.com/*

CSIRT TELCONET. Google lanza parche masivo para Chrome que corrige 429 vulnerabilidades. *https://csirt.telconet.net/comunicacion/boletines-servicios/google-lanza-parche-masivo-para-chrome-que-corrige-429-vulnerabilidades/*

CSIRT TELCONET. Actualización de seguridad en Google Chrome corrige vulnerabilidad Zero-Day en motor V8. *https://csirt.telconet.net/comunicacion/boletines-servicios/actualizacion-de-seguridad-en-google-chrome-corrige-vulnerabilidad-zero-day-en-motor-v8/*

SECURITYWEEK. Chrome 149 Patches 429 Vulnerabilities. *https://www.securityweek.com/chrome-149-patches-429-vulnerabilities/*

THE HACKER NEWS. AI Agent Uncovers 21 Zero-Days in Security Research. *https://thehackernews.com/2026/06/ai-agent-uncovers-21-zero-days-in.html*