Nro. Alerta:	AL-2026-045	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	7-sep-2026	Vulnerabilidad crítica de día cero en Google Chrome explotada activamente – CVE-2026-85046	Pág.: **1** of **4**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Ejecución de código / Explotación de vulnerabilidad
Nivel de riesgo: Alta

II. ALERTA

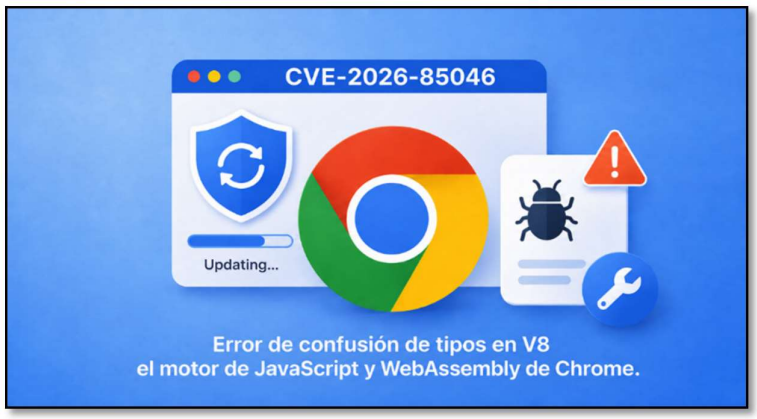

Figura 1.- Vulnerabilidad crítica de día cero en Google Chrome explotada activamente – CVE-2026-85046 - Figura referencial

Google ha publicado una actualización de seguridad de emergencia para Chrome tras el descubrimiento de una vulnerabilidad crítica de día cero (0-day), identificada como CVE-2026-85046. Se trata de una falla de confusión de tipos (CWE-843: Type Confusion) en el motor V8 de JavaScript y WebAssembly, que podría permitir a un atacante ejecutar código arbitrario en el navegador mediante contenido web malicioso, sin requerir interacción adicional por parte del usuario.

III. INTRODUCCIÓN

La vulnerabilidad CVE-2026-85046 es una falla de confusión de tipos (CWE-843: Type Confusion), que ocurre cuando un programa interpreta un objeto o dato como si perteneciera a un tipo diferente al que realmente es. Esta condición puede provocar accesos o manipulaciones incorrectas de memoria y en determinadas circunstancias, derivar en la corrupción de memoria y la ejecución de código arbitrario.

La vulnerabilidad afecta al motor V8 de JavaScript y WebAssembly de Google Chrome y podría permitir a un atacante remoto ejecutar código arbitrario dentro del sandbox de

Chrome (entorno aislado) mediante una página web HTML especialmente diseñada, una vez que el usuario accede a ella y sin interacción adicional.

En motores de JavaScript como V8, las suposiciones incorrectas sobre los tipos de objetos pueden resultar especialmente peligrosas, ya que las rutas de compilación altamente optimizadas dependen de información precisa sobre cómo se representan los arrays y objetos en la memoria.

IV. VECTOR DE ATAQUE

CVE-2026-85046 posee una severidad CRÍTICA, con una puntuación CVSS de 8.8 y el siguiente vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Los detalles de la vulnerabilidad fueron dadas a conocer a Google por el investigador Alvatore Gulizia, también conocido como Serotav, quien explicó que la falla reside en el comportamiento del compilador del motor V8, donde un array que contiene PACKED_ELEMENTS puede recibir incorrectamente un mapa PACKED_SMI_ELEMENTS. Esta discrepancia puede transformarse en accesos arbitrarios de lectura y escritura dentro del montón de JavaScript.

Google sin embargo ha restringido temporalmente el acceso al informe de errores de Chromium mientras la mayoría de los usuarios recibe la actualización de seguridad. Esta es una práctica habitual en la divulgación de vulnerabilidades de Chrome que están siendo explotadas activamente, ya que publicar detalles técnicos completos de forma prematura podría facilitar que otros atacantes realicen ingeniería inversa de la corrección y desarrollen exploits para aprovechar la vulnerabilidad.

El escenario típico de explotación inicia cuando un usuario sigue un enlace de phishing, se encuentra con un anuncio malicioso o visita un sitio web legítimo que ha sido comprometido. El contenido JavaScript o HTML manipulado podría entonces provocar una confusión de tipos en el motor V8, haciendo que Chrome realice operaciones basándose en suposiciones incorrectas sobre la representación de los objetos en la memoria.

V. IMPACTO

Navegadores Afectados	Versión vulnerable	Versión actualizable
Google Chrome (Windows & macOS)	Anterior a 152.0.7977.82	152.0.7977.82/.83 o superior
Google Chrome (Linux)	Anterior a 152.0.7977.82	152.0.7977.82 o superior
Microsoft Edge, Brave, Opera, Vivaldi	Todas las versiones que utilizan Chromium sin parches	Últimas actualizaciones de la versión estable

Tabla 1.- Servicios afectados - Vulnerabilidad crítica de día cero en Google Chrome explotada activamente – CVE-2026-85046 - Figura referencial

VI. INDICADORES DE COMPROMISO

Ante cualquier actividad sospechosa en el navegador considerar los siguientes indicadores:

- Procesos inesperados iniciados desde el árbol de procesos de Chrome.
- Alertas de posible explotación del navegador generadas por herramientas EDR o soluciones de protección de endpoints.
- Comportamientos sospechosos compatibles con corrupción de memoria relacionados con Chrome o V8.
- Visitas a sitios web recién registrados, comprometidos o conocidos por distribuir contenido malicioso inmediatamente antes de detectar actividad anómala.
- Ejecución inesperada de archivos ejecutables o scripts después de una sesión del navegador.
- Intentos de explotar una segunda vulnerabilidad después de una posible explotación del motor de renderizado de Chrome.
- Nueva actividad de persistencia o escalada de privilegios que ocurre inmediatamente después de detectar un comportamiento sospechoso del navegador.

VII. RECOMENDACIONES

- Se recomienda a los usuarios de Chrome que apliquen la actualización tan pronto como esté disponible, accediendo a Configuración > Acerca de Chrome y esperando a que la actualización se descargue e instale y luego reinicie el Chrome.

- Se recomienda una acción similar para los usuarios de navegadores basados en Chrome, incluidos Microsoft Edge, Brave, Opera y Vivaldi
- Restringir el acceso a sitios peligrosos hasta que se apliquen las actualizaciones.

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. (2026). *Vulnerabilidad crítica de día cero en Google Chrome explotada activamente.* https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-de-dia-cero-en-google-chrome-explotada-activamente/

SOC PRIME. (2026). *CVE-2026-85046 Analysis.* https://socprime.com/blog/cve-2026-85046-analysis/

THE HACKER NEWS. (2026). *Google Releases Chrome Update to Patch Critical Zero-Day Vulnerability.* https://thehackernews.com/2026/09/google-releases-chrome-update-to-patch.html

BLEEPINGCOMPUTER. (2026). *Google Warns of New Chrome Zero-Day Flaw Exploited in Attacks.* https://www.bleepingcomputer.com/news/security/google-warns-of-new-chrome-zero-day-flaw-exploited-in-attacks/

DEV.TO. (2026). *Chrome CVE-2026-85046: V8 Type Confusion Vulnerability Actively Exploited.* https://dev.to/anoymask/chrome-cve-2026-85046-v8-type-confusion-vulnerability-actively-exploited-20od