Incidente ID:	0016
Fecha del reporte:	21/11/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad de Chrome
Herramienta de detección	N/A
Activo involucrado:	Google Chrome
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del Ecosistema Digital sobre la vulnerabilida CVE-2025-13223 en el motor V8 de JavaScript y WebAssembly, el componente central que impulsa al navegador Google Chrome y otros navegadores basados en Chromium.

Descripción:

Se ha identificado una vulnerabilidad alta con calificación CVSS 8.8, explotada activamente como un ataque Zero-day, el problema reside en un error de «confusión de tipos» (Type Confusion) dentro del motor V8 de JavaScript. Este tipo de vulnerabilidad es particularmente peligrosa y codiciada por los atacantes. Ocurre cuando el software intenta acceder a un recurso (como un objeto en la memoria) utilizando un tipo de datos incorrecto. Un atacante puede diseñar una página web maliciosa que, al ser procesada por el navegador de una víctima, explota esta confusión para corromper la memoria del sistema (un 'heap corruption').

El objetivo final de esta manipulación de la memoria es lograr la ejecución arbitraria de código (RCE). En términos prácticos, esto significa que un atacante podría ejecutar comandos en el ordenador de la víctima con los mismos privilegios que el navegador, lo que podría llevar al

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

robo de información sensible, la instalación de malware (como ransomware o spyware) o la toma de control total del sistema afectado

Google destaca la gravedad de la vulnerabilidad y pide a todos los usuarios de Chrome actualizar cuanto antes. La compañía ya ha lanzado parches para las versiones en Windows y macOS (con número de versión 142.0.7444.175) y Linux (con número de versión 142.0.7444.176).

Productos afectados:

Esta vulnerabilidad afecta a todos los navegadores que utilizan el motor V8 de Chromium anteriores a la actualización de seguridad de noviembre de 2025.

- Google Chrome: Versiones anteriores a 142.0.7444.175 (Linux/Windows) y 142.0.7444.176 (macOS).
- Microsoft Edge: Versiones basadas en el núcleo Chromium afectado.
- Brave Browser: Versiones desactualizadas.
- Opera / Vivaldi: Versiones desactualizadas.

Modo de explotación y cadena de infección

V8 utiliza un sistema de optimización llamado TurboFan. JavaScript es un lenguaje dinámico (los tipos pueden cambiar), pero para que sea rápido, V8 hace "suposiciones especulativas" sobre los tipos de datos. Si una función se ejecuta mil veces con un "Array de Enteros", TurboFan compila esa función a código máquina asumiendo que *siempre* será un Array de Enteros, eliminando las comprobaciones de seguridad para ganar velocidad.

La vulnerabilidad ocurre cuando el atacante logra cambiar el tipo de un objeto después de que V8 ha realizado las comprobaciones de seguridad, pero antes de que acceda a la memoria.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Esto generalmente se logra a través de JIT (Just-In-Time) Optimization bugs.

Crean una función que toma un arreglo (Array) y accede a sus elementos. Se llama a esta función miles de veces con un arreglo de números de punto flotante (Double Array). V8 optimiza la función asumiendo que el arreglo siempre contiene Doubles.

El atacante invoca la función una vez más, pero esta vez utiliza un truco (como un *callback* o un *getter* malicioso) para cambiar el tipo del arreglo en medio de la ejecución. El arreglo se convierte, por ejemplo, en un arreglo de Objetos (Object Array).

El código optimizado de TurboFan no se da cuenta del cambio. Intenta leer o escribir en el arreglo pensando que son Doubles, pero en realidad está manipulando punteros de objetos en el *Heap*.

Recomendaciones de mitigación:

Dado que Google ha confirmado que ya existen exploits funcionando para esta vulnerabilidad, la acción requerida es inmediata.

- Actualización Inmediata: Forzar la actualización del navegador a la versión parcheada más reciente.
    - Para Chrome: Ir a *Menú (tres puntos) > Ayuda > Información de Google Chrome*. El navegador buscará e instalará la actualización automáticamente.
    - Versión Segura Mínima: Asegúrese de que la versión instalada sea 142.0.7444.175 o superior.

Reinicio del Navegador: La actualización no surte efecto hasta que el navegador se reinicia por completo.

- Gestión de Parches por políticas: Los administradores de sistemas deben desplegar la actualización mediante políticas de grupo (GPO) o herramientas de gestión de dispositivos (MDM) de forma prioritaria a todos los *endpoints*.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Desconfiar del Phishing: Los atacantes saben que esta noticia es pública. Es probable que surjan campañas de phishing (correos electrónicos, pop-ups) que simulen ser «actualizaciones urgentes de Chrome». Nunca descargue Chrome desde un enlace en un correo. La única forma segura de actualizar es a través del menú interno del propio navegado

Fuentes:

- https://www.softzone.es/noticias/seguridad/actualizar-chrome-vulnerabilidad-cve13223/
- https://hipertextual.com/tecnologia/google-avisa-de-un-grave-fallo-en-chrome-que-te-puede-estar-afectando-sin-que-lo-sepas-asi-puedes-protegerte/
- https://www.adslzone.net/
- https://devel.group/blog/google-corrige-un-nuevo-zero-day-explotado-en-chrome-cve-2025-13223/
- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-zero-day-en-google-chrome-activamente-explotada/
- https://www.cve.org/CVERecord?id=CVE-2025-13223

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570