

Incidente ID:	0066
Fecha del reporte:	04/12/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Actualización de Chrome a la versión 143
Herramienta de detección	N/A
Activo involucrado:	Chrome
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Medio

Objetivo:

Informar a las entidades del Ecosistema Digital sobre la actualización de Google lanzando la versión 143.0.7499.40 para Linux y 143.0.7499.40/41 para Windows y Mac.

Esta importante actualización aborda 13 vulnerabilidades de seguridad, incluidas varias fallas de alta gravedad que podrían permitir a los atacantes ejecutar código arbitrario o comprometer el motor de renderizado del navegador.

Descripción:

Google ha lanzado oficialmente Chrome 143 para el canal estable en todas las plataformas de escritorio principales. Esta actualización no es meramente estética ni funcional; es un parche de seguridad vital.

La nueva versión corrige 13 vulnerabilidades de seguridad. Entre ellas, los investigadores y el equipo de Google han identificado fallos de gravedad alta que podrían comprometer la integridad de tu equipo.

Las vulnerabilidades parcheadas afectan directamente al motor de renderizado del navegador y, lo que es más preocupante, cierran puertas que permitían la Ejecución Remota de Código (RCE).

La vulnerabilidad más crítica abordada en esta versión es CVE-2025-13630, una vulnerabilidad de confusión de tipos en el motor JavaScript V8.

En un contexto de navegador, la explotación exitosa de un error de confusión de tipo V8 a menudo permite a un atacante remoto ejecutar código arbitrario dentro del entorno limitado del renderizador engañando al usuario para que visite un sitio web especialmente diseñado.

Otro problema de alta gravedad es CVE-2025-13631, una falla de implementación inapropiada en el servicio Google Updater

La siguiente tabla resume las principales contribuciones de seguridad externa resueltas en Chrome 143:

CVE ID	Severidad	Tipo de Vulnerabilidad	Componente
CVE-2025-13630	High	Type Confusion	V8
CVE-2025-13631	High	Inappropriate Implementation	Google Updater
CVE-2025-13632	High	Inappropriate Implementation	DevTools
CVE-2025-13634	Medium	Inappropriate Implementation	Downloads
CVE-2025-13635	Low	Inappropriate Implementation	Downloads
CVE-2025-13636	Low	Inappropriate Implementation	Split View



Impacto Operativo:

Para entender la gravedad, se dividió en los dos riesgos principales que esta actualización elimina:

- Ejecución Remota de Código (RCE):

Estas vulnerabilidades suelen derivar de fallos en la gestión de memoria, específicamente errores de tipo Use-After-Free (UAF) o Heap Buffer Overflow. Un atacante puede manipular la asignación de memoria del navegador inyectando un *payload* malicioso en un segmento de memoria liberado o desbordado.

Si el exploit tiene éxito, el atacante logra secuestrar el flujo de control de la aplicación. Esto permite la ejecución de instrucciones de máquina (shellcode) dentro del contexto de seguridad del usuario actual sin interacción adicional. En escenarios avanzados, esto puede encadenarse con una vulnerabilidad de "escape de sandbox" para ganar persistencia en el sistema operativo anfitrión.

- Compromiso del Motor de Renderizado:

El motor de renderizado (Blink) y el motor de JavaScript (V8) son objetivos frecuentes. Las vulnerabilidades aquí a menudo implican Type Confusion (confusión de tipos) en V8, donde el motor interpreta un puntero de memoria de manera incorrecta (por ejemplo, tratar un entero como un objeto).

Denial of Service (DoS): Corrupción de estructuras críticas del DOM que fuerza el cierre inesperado del proceso renderer.

Al comprometer el motor que "dibuja" la web, un atacante puede eludir la Política del Mismo Origen (SOP), inyectando scripts maliciosos que el navegador interpreta como legítimos, permitiendo la exfiltración de cookies de sesión o tokens de autenticación.

Versiones Afectadas:

La nueva versión estable de Chrome está disponible como:

- 143.0.7499.40 para Linux
- 143.0.7499.40/41 para Windows y macOS
- 143.0.7499.52 para Android
- 143.0.7499.92 para iOS

Recomendaciones:

- La mayoría de los navegadores se actualizan automáticamente en segundo plano, pero dada la gravedad de estos 13 fallos, se recomienda forzar la verificación manual de la siguiente forma:
 - Para Chrome: Ir a Menú (tres puntos) > Ayuda > Información de Google Chrome. El navegador buscará e instalará la actualización automáticamente.

El navegador buscará la actualización Chrome 143. Si está disponible, comenzará a descargarla.

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.



Fuentes:

- 
- <https://proenseguridad.com/amenazas-online/vulnerabilidades/google-chrome-143-lanza-parches-para-13-vulnerabilidades-criticas/>
 - https://developer.chrome.com/release-notes/143?hl=es_419
 - <https://www.pcworld.com/article/2998949/chrome-143-fixes-13-security-flaws-plus-new-read-aloud-and-ai-features.html>

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.

