

Alerta ID:	0025
Fecha del reporte:	04/09/2025
Entidad:	N/A
Título:	Google corrige vulnerabilidades de alta gravedad de Chrome en su última actualización.
Herramienta de detección	securityweek
Activo involucrado:	Equipos de escritorio y portátiles donde esté instalado el navegador
Tipo de alerta:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del Ecosistema Digital sobre la actualización de seguridad publicada por Google el martes 2 de septiembre de 2025, en la cual se corrigen seis (6) vulnerabilidades, una de ellas de alta gravedad con el fin de promover la pronta aplicación de parches y reducir el riesgo de explotación en los navegadores Chrome y otros basados en Chromium. Dentro de las vulnerabilidades identificadas se detectó el **CVE-2025-9864** que tiene un nivel crítico para el sistema operativo.



Riesgo:

Las vulnerabilidades identificadas permiten explotar los navegadores de Chrome generando robo de información, inyección de código, ejecución de malware, modificación no autorizada de información y denegación de la operación del sistema operativo.

Actualizar a la versión 140 publicada por Google (2 de Septiembre 2025)



La actualización a la versión 140 de Google Chrome corrige seis (6) vulnerabilidades de seguridad identificadas en el navegador.

La vulnerabilidad más crítica es la **CVE-2025-9864**, una vulnerabilidad de uso después de la liberación de alta severidad en el motor JavaScript V8, reportada por el equipo de seguridad de Yandex. Este tipo de falla de corrupción de memoria ocurre cuando el código JavaScript accede a objetos después de que su memoria ha sido desasignada, lo que puede derivar en corrupción de la memoria dinámica (heap) y en algunos casos puede permitir la ejecución remota de código (RCE).

Las demás vulnerabilidades corregidas incluyen fallas de gravedad media en distintos componentes de Chrome, como la barra de herramientas, las extensiones y el módulo de descargas, las cuales fueron reportadas por investigadores externos.

Recomendaciones de actualización:



Si bien Google no menciona que ninguna de estas vulnerabilidades haya sido explotada, si recomienda a los usuarios que actualicen sus navegadores lo antes posible.

La última versión de Chrome ya está disponible como la versión 140.0.7339.80/81 para Windows y macOS. De igual manera, la última versión de Chrome ya está disponible como la versión 140.0.7339.80 para Linux.



Pasos para la actualización:



1. Ingresar a la página oficial de descargas de Google Chrome:
 - https://chromeenterprise.google/intl/es-419_ALL/download/?utm_source
2. Hacer clic en el botón Descargar Chrome.
3. Seleccionar el sistema operativo correspondiente.
4. Seleccionar Canal, Seleccionar Estable.
5. Seleccionar Tipo de archivo, seleccionar: Paquete (si la instalación será manual en un equipo individual) o MSI (si el despliegue se realizará en entornos administrados o de manera masiva)
6. Seleccionar la arquitectura del sistema operativo (32 o 64 bits).
7. Hacer clic en Aceptar y descargar.
8. Se iniciará la descarga del instalador.
9. Una vez completada, ejecuta el archivo descargado para comenzar la instalación.
10. Tras finalizar la instalación, verificar que la versión 140 esté instalada, ingresando en la barra de direcciones:
 - `chrome://settings/help`



Fuentes:



- <https://www.securityweek.com/google-patches-high-severity-chrome-vulnerability-in-latest-update/>
- https://chromeenterprise.google/intl/es-419_ALL/download/?utm_source

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.

