Boletín informativo
Vulnerabilidad en componente WebView de Chrome

CSIRTSALUD-AV-20260107-22 **TLP: CLEAR**

Incidente ID:	0022
Fecha del reporte:	07/01/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad en componente WebView 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 vulnerabilidad de nivel alta (cvss: 8.8) con código CVE-2026-0628 la cual se clasifica como una aplicación insuficiente de políticas (*Insufficient policy enforcement*) en el componente de la etiqueta WebView de Google Chrome.

Descripción:

Google ha corregido una vulnerabilidad en las nuevas versiones de Chrome 143.0.7499.192 para Windows y macOS, y 143.0.7499.192 para Linux. Según Google, esta vulnerabilidad aún no se ha explotado activamente.

Esta vulnerabilidad que afecta el componente WebView el cual es crucial de Chrome, permite a las aplicaciones mostrar contenido web dentro de sus interfaces sin iniciar un navegador completo.

Una calificación de esta gravedad significa que los atacantes podrían eludir los controles de seguridad, lo que provocaría acceso no autorizado, fugas de datos o la ejecución de código malicioso en aplicaciones que utilizan WebView.

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

Productos afectados:

La vulnerabilidad afecta a todas las versiones de Google Chrome anteriores a la 143.0.7499.192. Específicamente en las siguientes plataformas:

- Windows: Versiones previas a 143.0.7499.192
- macOS: Versiones previas a 143.0.7499.192
- Linux: Versiones previas a 143.0.7499.192
- Android: Versiones previas a 143.0.7499.192

Modo de explotación y cadena de infección

la etiqueta WebView de Chrome no aplicaba correctamente sus políticas de seguridad. Las extensiones usan WebView para incrustar contenido web, pero se supone que existe un aislamiento sólido. El error implicaba que una extensión podía eludir algunos de esos límites. Se trata de una falla en los límites de confianza. WebView, en lugar de contener estrictamente su contenido, permitía que la información manipulada se filtrara a áreas más sensibles.

En términos más simples la falla permite romper el aislamiento de seguridad entre una página web cargada en un WebView y las páginas privilegiadas del navegador (como chrome://settings o páginas internas de extensiones).

Mecanismo de Explotación:

El atacante utiliza técnicas de ingeniería social para convencer al usuario de instalar una extensión de Chrome maliciosa o visitar un sitio que interactúa con una aplicación que utiliza WebViews vulnerables.

Una vez que la extensión está activa, aprovecha la falta de validación de políticas en la etiqueta <webview> para inyectar scripts (JavaScript) o código HTML en páginas que normalmente están protegidas.

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

Al lograr ejecutar código en una página privilegiada, el atacante puede acceder a datos sensibles, modificar configuraciones del navegador o incluso intentar un escape del sandbox.

El uso de esta vulnerabilidad suele alinearse con las siguientes tácticas y técnicas:

- T1566 (Phishing): Para la distribución inicial de la extensión o el enlace malicioso.
- T1176 (User Installed Extensions): El atacante engaña al usuario para que instale una extensión que contiene el exploit.
- T1059.007 (JavaScript/JScript): Inyección de scripts para manipulación del DOM y robo de cookies o tokens.
- T1548 (Abuse Elevation Control Mechanism): Intento de saltar restricciones de seguridad del navegador para obtener mayores privilegios.

Recomendaciones de mitigación:

La única solución definitiva es la actualización del motor Chromium a la versión corregida.

- Actualización Manual
    - Ir a *Menú (tres puntos) > Ayuda > Información de Google Chrome*. El navegador buscará e instalará la actualización automáticamente.
    - Versión Segura: Asegúrese de que la versión instalada sea 143.0.7499.193 para Windows y Mac.

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*.

- Revisar y eliminar extensiones que no provengan de fuentes confiables o que no sean necesarias para la operación.

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

Fuentes:

- https://cybersecuritynews.com/chrome-webview-vulnerability/
- https://csirt.telconet.net/comunicacion/boletines-servicios/actualizacion-urgente-de-seguridad-en-chrome-para-vulnerabilidad-critica-en-webview/
- https://chromereleases.googleblog.com/2026/01/stable-channel-update-for-desktop.html
- https://www.tenable.com/plugins/nessus/281894
- https://www.forbes.com/sites/daveywinder/2026/01/07/google-chrome-143-security-bypass---3-billion-users-at-risk/
- https://www.cybersecurity-help.cz/vdb/SB2026010658

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