Alerta en Google: emiten una segunda advertencia por ataques al navegador Chrome

06/04/2026

Google emitió una nueva alerta de seguridad para usuarios de Chrome tras confirmar que ciberdelincuentes explotaron una falla, la segunda advertencia en apenas días. El fallo, bautizado CVE-2026-5281, es una vulnerabilidad de Chrome cero día que permitió ataques antes de que el parche estuviera disponible para la mayoría de los equipos.

Un fallo cero día significa que el proveedor no conoce la vulnerabilidad y no tuvo días para remediarla, por eso resulta tan peligrosa. Google indicó que la falla afecta al componente Dawn WebGPU, encargado de traducir instrucciones gráficas complejas entre dispositivos, lo que facilita visuales y cálculos avanzados en la web.

Qué dice Google

“El acceso a los detalles del fallo y los enlaces puede mantenerse restringido hasta que la mayoría de los usuarios estén actualizados con una corrección”, dijo Srinivas Sista, del equipo de Chrome. **Google explicó que suele limitar la información pública hasta que el parche llegue masivamente**, lo que explica la escasez de detalles técnicos en el anuncio.

Qué puede pasar

Si un atacante logra explotar CVE-2026-5281 puede corromper datos, provocar caídas del **sistema y ejecutar código malicioso** mediante una página HTML trampa. **Google lanzó un parche para esta vulnerabilidad y otras veinte más,** pero la compañía advirtió que la distribución del arreglo puede tardar semanas, dejando a usuarios expuestos durante el despliegue.

Los usuarios pueden adelantarse y actualizar manualmente Chrome: entrar al menú de tres puntos, ir a «Ayuda» y elegir «Acerca de **Google Chrome**». Allí el navegador buscará e instalará actualizaciones pendientes automáticamente. Tras la instalación es clave reiniciar el navegador para que el parche quede aplicado y minimizar la ventana de oportunidad para los explotadores.

No es la primera vez este año: el 13 de marzo Google difundió actualizaciones urgentes para corregir otros dos zero-day, CVE-2026-3909 y CVE-2026-3910. Esas fallas también podían afectar la integridad de datos y la disponibilidad de sistemas, por lo que empresas y administradores de TI tuvieron que acelerar los parches para evitar brechas mayores.

Con cerca de 3.500 millones de instalaciones de Chrome, la **vulnerabilidad de Chrome** CVE-2026-5281 pone en relieve la necesidad de mantener navegadores al día y revisar políticas de seguridad. Mientras **Google despliega fixes, conviene**

revisar extensiones y sistemas operativos, y mantener backups actualizados para limitar el daño si algún equipo resultara comprometido.

Fuente: La 100