Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

GOOGLE PUBLICA ACTUALIZACIÓN DE SEGURIDAD PARA CHROME ANTE VULNERABILIDAD CRÍTICA EN EXPLOTACIÓN ACTIVA

20/ 05 / 2025

CONTENIDO

Introducción

En el dinámico panorama de las amenazas cibernéticas, la velocidad de respuesta ante vulnerabilidades críticas marca una diferencia significativa en la protección de datos y activos digitales. El 19 de mayo de 2025, Google emitió una actualización de seguridad urgente para su navegador Chrome, dirigida a mitigar una falla de seguridad ya identificada como explotada en entornos reales. Esta vulnerabilidad, catalogada como CVE-2025-4664, afecta directamente la integridad del proceso de carga de recursos web y expone a los usuarios al robo de información sensible.

Dado que Chrome es ampliamente utilizado tanto en entornos personales como corporativos, este incidente subraya la importancia de mantener una postura proactiva frente a actualizaciones de seguridad críticas. A continuación, se detallan los aspectos técnicos, el impacto potencial y las recomendaciones clave para usuarios y administradores de TI.

GOOGLE PUBLICA ACTUALIZACIÓN DE SEGURIDAD PARA CHROME ANTE VULNERABILIDAD CRÍTICA EN EXPLOTACIÓN ACTIVA

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_05_20_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	20/05/2025
Es día cero (0 day):	No

RESUMEN

Google ha lanzado una actualización de emergencia para su navegador Chrome, abordando una vulnerabilidad crítica que ya está siendo explotada activamente. Esta falla, identificada como CVE-2025-4664, puede poner en riesgo información sensible de los usuarios y permitir a atacantes robar credenciales o tomar control de cuentas.

¿Qué versiones están afectadas?
La actualización eleva el canal Stable de Chrome a las versiones:

- **Windows y macOS: 136.0.7103.113 / .114**
- **Linux: 136.0.7103.113**

Si usas Chrome y no has cerrado tu navegador en varios días, o si alguna extensión impide su actualización automática, podrías estar en riesgo sin saberlo.

¿Cómo actualizar Chrome manualmente?
Para asegurarte de estar protegido:

1. **Abre Chrome.**
2. **Ve a Configuración > Acerca de Chrome.**
3. **Si hay una actualización disponible, Chrome la descargará automáticamente.**
4. **Reinicia el navegador para aplicar el parche.**

La versión segura confirmada es 136.0.7103.114.

¿Por qué es tan grave esta vulnerabilidad?

La vulnerabilidad afecta al componente Chrome Loader, encargado de gestionar las solicitudes de recursos al visitar un sitio web (como imágenes, scripts o estilos).

En condiciones normales, Chrome aplica políticas de seguridad que impiden que un sitio web acceda a información de otro, lo que se conoce como "same-origin policy". Sin embargo, debido a un error, estas políticas no se aplicaban correctamente a los encabezados de tipo Link.

Esto permitía a un atacante configurar un encabezado malicioso que instruye al navegador a incluir URLs completas con parámetros sensibles, como tokens OAuth o identificadores de sesión.

Ejemplo de ataque: robo de tokens sin interacción

Imagina que accedes a un sitio bancario o una plataforma con información sensible. Si la URL contiene un token o código secreto para autenticarte, un atacante podría incrustar un recurso invisible (como una imagen) en una página o anuncio, y extraer ese token sin que lo notes.

Esto puede facilitar:

- Robo de cuentas
- Suplantación de identidad
- Acceso no autorizado a servicios personales o corporativos

Confirmación de explotación activa

Aunque Google no ha confirmado directamente la explotación activa del fallo, la CISA (Cybersecurity and Infrastructure Security Agency) ha agregado esta vulnerabilidad a su catálogo de Vulnerabilidades Conocidas y Explotadas, lo que indica un riesgo real y presente.

Recomendaciones

- Actualiza Chrome inmediatamente en todos tus dispositivos.
- Refuerza la gestión de sesiones sensibles (por ejemplo, rotando tokens de autenticación).
- Si administras una red corporativa, considera forzar la actualización en estaciones de trabajo mediante políticas de grupo o herramientas MDM.

Conclusión

Esta vulnerabilidad demuestra cómo una falla técnica aparentemente menor puede tener consecuencias graves para la seguridad de los usuarios. Mantener navegadores actualizados es una práctica crítica para proteger tanto a individuos como a organizaciones.

NOTICIA COMPLETA

https://devel.group/blog/google-publica-actualizacion-de-seguridad-para-chrome-ante-vulnerabilidad-critica-en-explotacion-activa/

CONTACTOS DE SOPORTE

Correo electrónico: soporte@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group/