Alerta de Seguridad

COLCERT AL-20250410-065

TLP:CLEAR

Vulnerabilidad Crítica en Google Chrome (CVE-2025-2783)

Se ha identificado una vulnerabilidad de día cero en el navegador Google Chrome, catalogada como CVE-2025-2783, que permite a los atacantes evadir el sandbox de seguridad del navegador. Esta vulnerabilidad también afecta a otros navegadores basados en Chromium, como Microsoft Edge, Opera, Brave y Vivaldi.

Recomendación: Debido a que en algunos casos la actualización automática no se realiza correctamente, **se recomienda realizar la actualización manualmente** para asegurar la protección contra esta vulnerabilidad.

La vulnerabilidad ha sido explotada activamente por actores de amenazas avanzados (APT) en una campaña de ciberespionaje conocida como Operación ForumTroll, dirigida principalmente a periodistas, universidades y entidades gubernamentales.

VULNERABILIDAD	CVE-2025-2783
IMPACTO	Ejecución remota de código, robo de información
AFECTA A	Google Chrome (todas las plataformas)
EXPLOTACIÓN ACTIVA	Confirmada
SOLUCIÓN	Actualizar a versión 134.0.6998.88/.89 o superior

Detalles Técnicos

- **Vector de ataque:** Documentos maliciosos o enlaces phishing enviados por correo electrónico.
- **Impacto:** Ejecución remota de código, robo de credenciales, persistencia en el sistema, fuga de información confidencial.
- **Malware asociado:** StilachiRAT – Un troyano avanzado que roba cookies de sesión, contraseñas almacenadas, información de billeteras criptográficas y realiza captura de pantalla del sistema comprometido.

¿Cómo actualizar Google Chrome manualmente?

Abre Google Chrome y sigue estos pasos.

1. Haz clic en el ícono de tres puntos verticales en la esquina superior derecha.
2. Selecciona "Ayuda" > "Información de Google Chrome".
3. Chrome buscará automáticamente actualizaciones. Si hay una disponible, se descargará de inmediato.
4. Una vez completada la descarga, haz clic en "Reiniciar" para aplicar la actualización.
5. Verifica que la versión instalada sea 134.0.6998.177 o superior.

StilachiRAT Ciberespionaje a Través de la Vulnerabilidad CVE-2025-2783 en Chrome:
El troyano StilachiRAT es una herramienta de acceso remoto (RAT) utilizada en campañas de ciberespionaje avanzadas. En el contexto de la vulnerabilidad CVE-2025-2783 de Google Chrome, fue desplegado mediante correos de phishing dirigidos, que explotaban esta falla para evadir el sandbox del navegador y ejecutar código malicioso en el sistema. Una vez instalado, StilachiRAT permite el control remoto del equipo, el robo de credenciales, cookies, billeteras digitales y la exfiltración silenciosa de información confidencial hacia servidores controlados por atacantes.

Alerta de Seguridad

Vulnerabilidad Crítica en Google Chrome (CVE-2025-2783)

COLCERT AL-20250410-065

TLP:CLEAR

Solución / Mitigación:

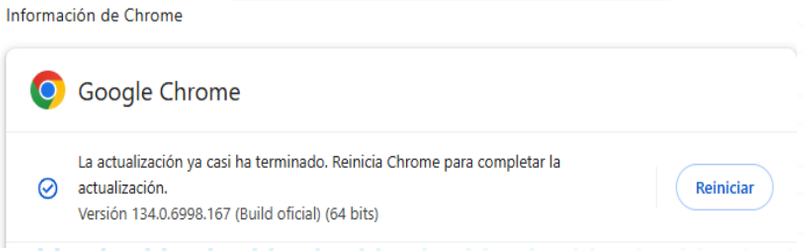
Google ha lanzado una actualización de seguridad urgente.

Actualizar inmediatamente a:

Google Chrome versión 134.0.6998.88/.89 (Windows/Mac/Linux) o superior.

También puedes acceder directamente escribiendo en la barra de direcciones:

chrome://settings/help



Flujo de Infección Explotando la Vulnerabilidad de Chrome (CVE-2025-2783)

Paso 1: Phishing con enlaces maliciosos
El atacante envía correos con enlaces falsos o adjuntos peligrosos para engañar al usuario.

Paso 2: Descarga de carga útil (Payload)
Al hacer clic, el usuario descarga un archivo malicioso que contiene la carga útil del atacante

Paso 3: Escape del entorno seguro (Sandbox Escape)
El malware aprovecha una vulnerabilidad del navegador para evadir el sandbox y ejecutarse en el sistema operativo.

Paso 4: Instalación de StilachiRAT
El troyano StilachiRAT se instala en el equipo, otorgando al atacante acceso remoto y persistente.

Paso 5: Robo de datos y exfiltración
El malware recopila credenciales, información confidencial y la transmite al servidor del atacante.

Técnicas comunes de persistencia y exfiltración

- Uso de PowerShell para ejecutar código embebido.
- Enumeración de procesos (tasklist), red (ipconfig /all) y entorno del usuario.
- Exfiltración de información por canales HTTP(S) cifrados.

Acceso a archivos como:

- Login Data (Chrome – SQLite de contraseñas)
- Cookies (Chrome – persistencia de sesión)
- Claves de wallet en %APPDATA% y %LOCALAPPDATA%

Fuente: Microsoft Incident Response: StilachiRAT

COLCERT

Alerta de Seguridad

Vulnerabilidad Crítica en Google Chrome (CVE-2025-2783)

COLCERT AL-20250410-065

TLP:CLEAR

Recomendaciones por roles

Usuarios finales:

- ❑ No hacer clic en correos o enlaces sospechosos.
- ❑ Mantener navegador y antivirus actualizados.

Administradores de sistemas:

- ❑ Forzar actualización vía GPO o políticas de grupo.
- ❑ Monitorizar actividad anómala en endpoints.
- ❑ Aislar equipos no actualizados.
- ❑ Realizar actualización manual.

Actualice los navegadores de inmediato y verifique posibles exposiciones.
Esta vulnerabilidad representa un alto riesgo para la seguridad de la información.

NIVEL DE RIESGO

ALTO

FUENTES:

1 **Blog oficial de actualizaciones de Chrome**
https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_25.html

2 **Informe sobre la campaña ForumTroll – NY Post**
https://nypost.com/2025/03/26/tech/google-chrome-confirms-cyber-espionage-attacks-from-highly-sophisticated-malware/

3 **Advertencia de Microsoft sobre StilachiRAT – MeriStation**
https://as.com/meristation/betech/microsoft-alerta-del-virus-que-roba-informacion-personal-desde-google-chrome-no-han-logrado-conocer-la-localizacion-del-culpable-n/