Boletín informativo
Vulnerabilidades críticas en Google Chrome

CSIRTSALUD-AV-20260317-36 **TLP: CLEAR**

Incidente ID:	036
Fecha del reporte:	19/03/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidades críticas en Google Chrome
Herramienta de detección	N/A
Activo involucrado:	Google Chrome
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Medio

Objetivo:

Informar a las entidades del Ecosistema sobre la alerta emitida por la Agencia de Ciberseguridad e Infraestructura de Estados Unidos (CISA) ha emitido una alerta urgente respecto a dos vulnerabilidades de día cero (zero-day) identificadas en Google Chrome y motores basados en Chromium, catalogadas como **CVE-2026-3909** y **CVE-2026-3910**. Ambas fallas están siendo explotadas activamente en entornos reales y han sido agregadas al catálogo de Vulnerabilidades Conocidas Explotadas (KEV) de CISA.

Descripción:

El 10 de marzo de 2026, el equipo de seguridad interno de Google identificó y reportó dos vulnerabilidades críticas en el motor de renderizado de Chrome. El 13 de marzo de 2026, CISA confirmó la explotación activa en entornos reales y agregó ambas CVE al catálogo KEV. Google respondió con una actualización de emergencia llevando Chrome a la versión 146.0.7680.75 / 146.0.7680.76.

CSIRT Salud

Boletín informativo
Vulnerabilidades críticas en Google Chrome

CSIRTSALUD-AV-20260317-36

TLP: CLEAR

Ambas vulnerabilidades presentan las siguientes características de ataque:

Característica	Detalle
Vector de ataque	Red (remoto) - No requiere acceso previo al sistema
Interacción requerida	Mínima - Solo visitar una página web maliciosa o comprometida
Privilegios requeridos	Ninguno - No se necesitan privilegios especiales
Complejidad del ataque	Baja - El exploit es sencillo de activar para el atacante
Impacto en confidencialidad	Alto - Posible robo de datos y credenciales
Impacto en integridad	Alto - Ejecución de código arbitrario
Impacto en disponibilidad	Alto - Inestabilidad o caída del sistema
Descubridor	Google Threat Intelligence Group (GTIG) - 10 marzo 2026
Patron de ataque	Drive-by download / Watering hole / Malvertising

CVE-2026-3909 - Out-of-Bounds Write en Google Skia

Skia es una biblioteca gráfica de código abierto desarrollada por Google que se encarga de renderizar texto, formas geométricas e imágenes en pantallas digitales. Es utilizada no solo por Chrome sino también por Android, Chrome OS, el framework Flutter y múltiples aplicaciones de escritorio.

La vulnerabilidad CVE-2026-3909 ocurre en el proceso de manejo de buffers de memoria durante la renderización gráfica. Específicamente:

- Skia asigna un buffer de memoria de tamaño fijo para almacenar datos gráficos (píxeles, vectores, glifos).
- Al procesar una página HTML con contenido gráfico especialmente construido, Skia escribe datos más allá del límite del buffer asignado.
- Esta escritura fuera de límites (OOB Write) corrompe estructuras de memoria adyacentes del proceso de renderizado.
- Un atacante puede controlar qué datos se escriben en esas posiciones de memoria, logrando manipular el flujo de ejecución del proceso.
- El resultado es la posibilidad de ejecutar código arbitrario en el contexto del renderizado de Chrome.

CVE-2026-3910 - Implementación Incorrecta en Chromium V8

V8 es el motor de JavaScript y WebAssembly de código abierto desarrollado por Google que alimenta el navegador Chrome y el runtime Node.js. Es uno de los componentes más complejos y críticos del ecosistema Chromium.

La vulnerabilidad CVE-2026-3910 reside en una implementación incorrecta dentro de V8:

- V8 no aplica correctamente las restricciones sobre los buffers de memoria cuando ejecuta ciertas secuencias de código JavaScript o WebAssembly.
- Un atacante puede elaborar una página HTML con JavaScript malicioso que explota esta falla para manipular operaciones de memoria de forma no autorizada.

- La explotación exitosa permite al atacante ejecutar código arbitrario dentro del sandbox del navegador Chrome.
- Aunque el sandbox limita el acceso inmediato al sistema operativo, este acceso es suficiente para robar información del contexto del navegador.
- En ataques avanzados, este acceso al sandbox es el primer eslabón de una cadena que puede llevar al compromiso total del sistema operativo.

La explotación exitosa de estas vulnerabilidades puede tener consecuencias graves y de amplio alcance:

- Ejecución remota de código arbitrario dentro del sandbox del navegador (Remote Code Execution - RCE).
- Corrupción de memoria del proceso de renderizado, lo que puede causar fallos del sistema o el navegador (Denial of Service).
- Acceso a regiones de memoria fuera de los límites permitidos (Out-of-Bounds Memory Access).
- Encadenamiento con otros exploits para lograr escapar del sandbox y comprometer el sistema operativo completo.
- Robo de credenciales y sesiones activas almacenadas en el navegador (cookies, tokens OAuth, contraseñas).
- Despliegue de malware sofisticado: info-stealers, loaders para ransomware, backdoors y troyanos de acceso remoto (RATs).
- Movimiento lateral dentro de la red corporativa si el atacante escapa del sandbox.
- Exfiltración de datos sensibles de la organización, incluyendo información financiera, propiedad intelectual y datos de clientes.
- Comprometimiento de cadena de suministro si el sistema afectado tiene acceso a sistemas de desarrollo o producción.

Modo de explotación y cadena de infección

La cadena de explotación de estas vulnerabilidades sigue un patrón bien definido conocido como 'drive-by download' o ataque de abrevadero (watering hole). A continuación se describe el flujo completo de un ataque típico:

Fase 1: Preparación y Entrega (Initial Access)

El atacante prepara el entorno de ataque mediante alguno de los siguientes vectores:

- Sitio web malicioso creado específicamente para contener el payload de explotación (página HTML con JavaScript o contenido Skia especialmente construido).
- Comprometimiento de un sitio web legítimo (watering hole) para inyectar el exploit sin levantar sospechas del usuario.
- Campaña de malvertising: anuncios digitales que redirigen a páginas de explotación.
- Correo electrónico de phishing con enlace a la página maliciosa (spear-phishing para objetivos específicos).

Fase 2: Ejecución del Exploit (Execution)

Cuando la víctima visita la URL comprometida con una versión vulnerable de Chrome:

- El navegador carga el contenido HTML/JS especialmente diseñado.
- Para CVE-2026-3909 (Skia): El contenido gráfico malicioso desencadena la escritura fuera de límites en la biblioteca Skia, corrompiendo estructuras de memoria del renderizador.
- Para CVE-2026-3910 (V8): El código JavaScript malicioso explota la implementación incorrecta del motor V8, logrando ejecución de código arbitrario dentro del sandbox del navegador.
- El exploit se activa instantáneamente en segundo plano, sin que el usuario perciba ninguna actividad anormal visible.

Fase 3: Ejecución dentro del Sandbox

Una vez que el exploit tiene éxito inicial:

- El atacante obtiene ejecución de código dentro del proceso sandboxed del renderer de Chrome.
- Desde ahí puede ejecutar scripts de reconocimiento para identificar el sistema operativo, versión de Chrome, usuarios logueados y privilegios disponibles.
- Se puede robar información del contexto del navegador: cookies de sesión, tokens, historial, datos autocomplete y credenciales guardadas.

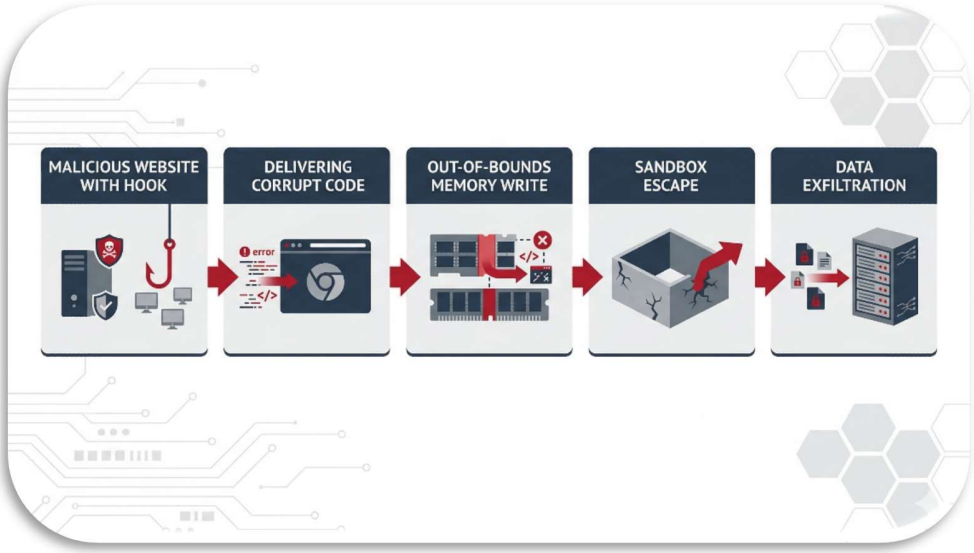
Fase 4: Escape del Sandbox (Privilege Escalation)

Esta es la fase más crítica del ataque avanzado:

- Los atacantes sofisticados encadenan (chain) el exploit de Chrome con una segunda vulnerabilidad de escape del sandbox (sandbox escape), como fallas en el kernel del SO o en IPC de Chromium (Mojo).
- Al escapar del sandbox, el atacante obtiene privilegios a nivel de proceso del sistema operativo.
- Esto permite escritura en el sistema de archivos, ejecución de procesos del sistema y acceso a redes corporativas internas.

Fase 5: Post-Explotación y Persistencia

- Descarga e instalación de payloads de segunda etapa: info-stealers, backdoors, loaders de ransomware.
- Establecimiento de mecanismos de persistencia (llaves de registro, tareas programadas, servicios del sistema).
- Movimiento lateral a otros sistemas de la red corporativa aprovechando credenciales robadas.
- Exfiltración de datos confidenciales hacia servidores de comando y control (C2) del atacante.

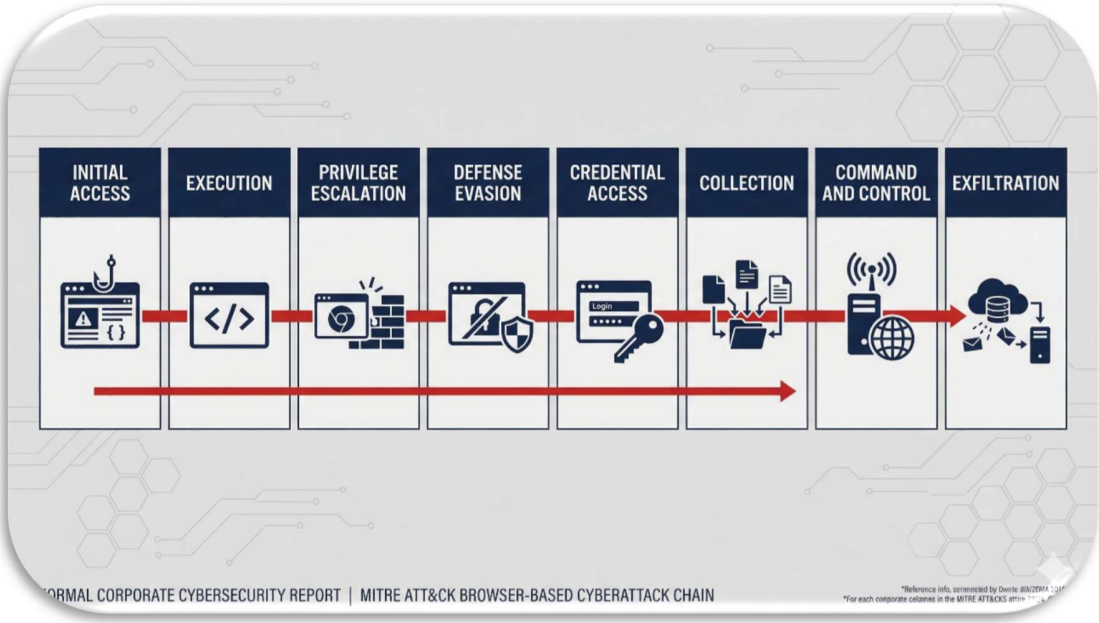


Relación con tácticas MITRE ATT&CK

Las vulnerabilidades CVE-2026-3909 y CVE-2026-3910 se alinean con múltiples tácticas y técnicas del framework MITRE ATT&CK:

Táctica ATT&CK	Técnica / Sub-técnica	Relación con el ataque
TA0001 - Acceso Inicial	**T1189 - Drive-by Compromise**	El usuario visita una página web maliciosa o comprometida que entrega el payload de explotación sin interacción adicional.
TA0002 - Ejecución	**T1203 - Exploitation for Client Execution**	Las CVE permiten la ejecución de código arbitrario en el proceso del renderer de Chrome mediante contenido web especialmente diseñado.
TA0004 - Escalada de Privilegios	**T1068 - Exploitation for Privilege Escalation**	Encadenamiento del exploit con una falla de escape del sandbox para obtener privilegios del sistema operativo anfitrión.

Táctica ATT&CK	Técnica / Sub-técnica	Relación con el ataque
TA0005 - Evasión de Defensas	**T1211 - Exploitation for Defense Evasion**	El ataque opera completamente dentro del proceso legítimo de Chrome, evadiendo controles de seguridad basados en procesos.
TA0006 - Acceso a Credenciales	**T1539 - Steal Web Session Cookie**	Acceso a cookies de sesión, tokens OAuth y credenciales almacenadas en el perfil del navegador.
TA0009 - Recolección	**T1185 - Browser Session Hijacking**	Captura de sesiones activas del navegador, historial, formularios autocomplete y datos de navegación.
TA0011 - C&C	**T1071.001 - Application Layer Protocol: Web Protocols**	Comunicación con servidores C2 del atacante usando tráfico HTTP/HTTPS que se mimetiza con tráfico legítimo del navegador.
TA0010 - Exfiltracion	**T1041 - Exfiltration Over C2 Channel**	Los datos robados son enviados al servidor del atacante a través del canal de C2 establecido.



Activos o versiones afectados:

Las vulnerabilidades afectan cualquier instalación de Google Chrome o motor Chromium anterior a la versión corregida:

- Google Chrome para Windows: Todas las versiones anteriores a 146.0.7680.75 / 146.0.7680.76
- Google Chrome para macOS: Todas las versiones anteriores a 146.0.7680.75 / 146.0.7680.76

Google Chrome para Linux: Todas las versiones anteriores a 146.0.7680.75

Navegadores Basados en Chromium Afectados

Dado que estos navegadores comparten el motor Chromium, están igualmente expuestos hasta que sus respectivos proveedores publiquen la actualización:

- Microsoft Edge (basado en Chromium)
- Opera
- Brave Browser
- Vivaldi
- Samsung Internet Browser
- Epic Privacy Browser
- Cualquier aplicación construida con el framework Electron que use una versión vulnerable de Chromium

Plataformas Adicionales Afectadas por Skia (CVE-2026-3909)

La biblioteca Skia es utilizada más allá del navegador, lo que amplía el alcance de la CVE-2026-3909:

- Chrome OS (ChromeOS) - Dispositivos Chromebook
- Android - Dispositivos móviles que utilizan Skia para renderización gráfica
- Aplicaciones desarrolladas con Flutter que usen Skia como backend de renderización
- Cualquier software de terceros que integre Skia como biblioteca de renderización

Indicadores de compromiso:

Dado que Google y CISA han restringido los detalles técnicos para evitar la proliferación del exploit, los indicadores publicados son de naturaleza comportamental. Se listan a continuación los patrones conocidos y observables:

Tráfico de red sospechoso asociado a explotación de Chrome:

- Peticiones HTTP/HTTPS a dominios con alto entropy en el nombre de dominio o subdominios inusuales.
- Descarga de archivos .html, .js o .wasm desde URLs no categóricas o de reciente registro (< 30 días).
- Tráfico POST hacía IPs externas desde el proceso chrome.exe / chrome inmediatamente después de visitar una página web.
- Comunicaciones salientes no habituales desde el proceso renderer o utility (procesos hijo de Chrome) hacía IPs externas.
- Uso de puertos inusuales en conexiones establecidas por procesos de Chrome (fuera de 80, 443, 8080).

Comportamientos sospechosos observables en el endpoint:

- Procesos hijo de chrome.exe / chrome que spawnan ejecutables del sistema (cmd.exe, powershell.exe, bash, sh).
- Escritura de archivos ejecutables (.exe, .dll, .sh, .py) desde el directorio temporal del navegador o perfil de usuario.
- Crash inesperado del renderizador de Chrome seguido de reconexión automática a la misma URL.
- Modificación o acceso no autorizado al keychain, credential store o directorio de perfil de Chrome.
- Aumento anormal de uso de CPU y memoria en el proceso del renderizador de Chrome al cargar una página específica.

- Presencia de archivos .html maliciosos en directorios de descarga con nombres aleatorios o codificados en base64.

Recomendaciones de mitigación:

- Actualizar Google Chrome a la versión 146.0.7680.75 o superior en todos los endpoints de la organización. Navegar a: Menú (tres puntos) > Ayuda > Información de Google Chrome.
- Actualizar Microsoft Edge, Brave, Opera y cualquier otro navegador basado en Chromium a sus versiones más recientes disponibles.
- Reiniciar completamente el navegador después de la actualización (el parche no es efectivo hasta que se reinicia).
- Verificar el despliegue del parche mediante herramientas de gestión de endpoints (MDM, SCCM, Intune) para confirmar cobertura total.

Actualizar aplicaciones Electrón y cualquier software que embebe el motor Chromium.

Controles Preventivos Adicionales:

- Activar las políticas de actualización automática de Chrome en toda la organización mediante Group Policy (Windows) o MDM profiles (macOS).
- Implementar listas de bloqueo de sitios web categóricos de alto riesgo en el proxy/firewall corporativo.
- Habilitar Safe Browsing Enhanced Protection en Chrome para todos los usuarios corporativos.
- Aplicar el principio de mínimo privilegio: los usuarios no deben ejecutar Chrome con privilegios de administrador.
- Evaluar el uso de aislamiento de sitios (Site Isolation) y contenedores de navegación para entornos de alto riesgo.
- Revisar y actualizar el inventario de aplicaciones que embeben motores Chromium (aplicaciones Electron, herramientas de desarrollo, etc.).

- Implementar políticas Zero-Trust de acceso a red que limiten el movimiento lateral en caso de compromiso de un endpoint.

Fuentes:

- **The Hacker News - Google Fixes Two Chrome Zero-Days Exploited in the Wild Affecting Skia and V8 (Mar. 13, 2026)**

https://thehackernews.com/2026/03/google-fixes-two-chrome-zero-days.html

- **SOC Prime - CVE-2026-3910: Chrome V8 Zero-Day Used for In-the-Wild Attacks**

https://socprime.com/blog/cve-2026-3910-vulnerability/

- **CVE Reports - CVE-2026-3909: Remote Code Execution via Out-of-Bounds Write in Google Skia**

https://cvereports.com/reports/CVE-2026-3909

- **Purple-Ops - CVE-2026-3909 and CVE-2026-3910 Chrome Fixes (CVSS 8.8)**

https://www.purple-ops.io/resources-hottest-cves/cve-2026-3909-3910-chrome/

- **Qualys ThreatPROTECT - Google Patches Two Chrome Vulnerabilities Exploited in the Wild (Mar. 16, 2026)**

https://threatprotect.qualys.com/2026/03/16/google-patches-two-chrome-vulnerabilities-exploited-in-the-wild-cve-2026-3909-cve-2026-3910/

- **Vulert Blog - Google Chrome Zero-Days CVE-2026-3909 & CVE-2026-3910 (Análisis técnico Skia y V8)**

https://vulert.com/blog/google-chrome-zero-days-cve-2026-3909-2026-3910/

- **CISA - Catálogo de Vulnerabilidades Conocidas Explotadas (KEV)**

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- **CISA - Alerta oficial: CISA Adds Two Known Exploited Vulnerabilities to Catalog (Mar. 2026)**

https://www.cisa.gov/news-events/alerts/2026/03/13/cisa-adds-two-known-exploited-vulnerabilities-catalog

- **MITRE ATT&CK Framework v18.1 (Marco de tácticas y técnicas adversariales)**
https://attack.mitre.org/

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.