

|                          |                                                                                                                                                                                                                        |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alerta ID:               | 110                                                                                                                                                                                                                    |
| Fecha del reporte:       | 18/06/2026                                                                                                                                                                                                             |
| Entidad:                 | Todas las entidades del ecosistema digital                                                                                                                                                                             |
| Título:                  | Explotación activa de vulnerabilidad Zero-Day en Google Chrome permite ejecución de código y compromiso de estaciones de trabajo institucionales                                                                       |
| Herramienta de detección | N/A                                                                                                                                                                                                                    |
| Activo involucrado:      | Google Chrome para Windows, Linux y macOS; navegadores basados en Chromium; estaciones de trabajo institucionales; equipos administrativos; plataformas clínicas accesibles vía navegador; servicios web corporativos. |
| Tipo de alerta:          | Alerta                                                                                                                                                                                                                 |
| Nivel de riesgo:         | Critico                                                                                                                                                                                                                |

### Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la explotación activa de la vulnerabilidad CVE-2026-11645 identificada en Google Chrome, la cual afecta el motor V8 encargado de procesar JavaScript y WebAssembly.

El propósito de esta alerta es que las entidades evalúen el impacto potencial que esta vulnerabilidad podría generar sobre:

- estaciones de trabajo institucionales;
- equipos administrativos y clínicos;
- plataformas web corporativas;
- sistemas de historia clínica electrónica;



- servicios de interoperabilidad;
- aplicaciones SaaS utilizadas por las entidades;
- servicios de autenticación institucional;
- y activos críticos accesibles mediante navegadores web.

Asimismo, se busca generar conciencia sobre los riesgos asociados a la navegación web, la exposición a sitios maliciosos, campañas de phishing y explotación de vulnerabilidades Zero-Day dirigidas a usuarios finales.

En el contexto del sector salud, este escenario representa un riesgo significativo debido a la alta dependencia de aplicaciones web utilizadas para soportar procesos asistenciales, administrativos y operativos.

#### Descripción:



Google confirmó la existencia y explotación activa de la vulnerabilidad CVE-2026-11645, una falla de seguridad de alta severidad identificada en el motor V8 de Google Chrome, componente responsable de la ejecución de código JavaScript y WebAssembly dentro del navegador.

De acuerdo con la información publicada por Google, la vulnerabilidad corresponde a un error de tipo Out-of-Bounds Read/Write, condición que se presenta cuando una aplicación accede a posiciones de memoria fuera de los límites asignados. Este tipo de debilidad puede permitir que un atacante manipule la memoria del proceso afectado, genere comportamientos inesperados y obtenga capacidades de ejecución de código arbitrario dentro del contexto del navegador comprometido.

Las investigaciones realizadas por Google permitieron establecer que la vulnerabilidad estaba siendo explotada activamente antes de la publicación de las actualizaciones de seguridad, lo que la clasifica como una vulnerabilidad Zero-Day. Este escenario incrementa significativamente el nivel de riesgo debido a que los actores maliciosos pueden aprovechar la



falla antes de que las organizaciones implementen las medidas de mitigación correspondientes.

La explotación de la vulnerabilidad puede producirse cuando un usuario accede a contenido web especialmente diseñado para activar la condición de corrupción de memoria presente en el motor V8. En escenarios de ataque, los ciberdelincuentes podrían utilizar sitios web comprometidos, campañas de phishing, enlaces maliciosos, publicidad maliciosa (malvertising) o recursos web controlados por atacantes para desencadenar la explotación de la vulnerabilidad.

Las evaluaciones técnicas indican que un atacante remoto podría:

- ejecutar código arbitrario dentro del navegador afectado;
- comprometer la integridad de las sesiones activas del usuario;
- acceder a información almacenada en memoria;
- obtener credenciales y tokens de autenticación;
- desplegar código malicioso adicional;
- descargar y ejecutar malware en el equipo comprometido;
- establecer mecanismos de persistencia;
- evadir controles de seguridad implementados en el navegador;
- y facilitar compromisos posteriores sobre la infraestructura institucional.

Uno de los aspectos más relevantes de esta vulnerabilidad corresponde a que Google Chrome es actualmente uno de los navegadores más utilizados dentro de los entornos corporativos, gubernamentales y del sector salud. Su uso generalizado para acceder a aplicaciones clínicas, plataformas administrativas, sistemas de historia clínica electrónica, servicios de interoperabilidad, herramientas de telemedicina y aplicaciones en la nube amplifica considerablemente la superficie de ataque disponible para los actores maliciosos.

En el contexto del sector salud, la explotación exitosa de esta vulnerabilidad podría afectar directamente estaciones de trabajo utilizadas por personal asistencial, administrativo y



tecnológico, permitiendo a los atacantes obtener acceso inicial a redes institucionales mediante técnicas orientadas al compromiso de usuarios finales.

Adicionalmente, debido a que la vulnerabilidad reside en uno de los componentes fundamentales del navegador, los atacantes podrían aprovecharla para ejecutar cargas maliciosas sin requerir privilegios elevados sobre el sistema operativo, facilitando la ejecución de actividades relacionadas con robo de información, espionaje cibernético, distribución de malware, secuestro de sesiones y movimiento lateral hacia otros activos de la organización.

Las organizaciones que utilizan Google Chrome o navegadores basados en Chromium deben considerar esta vulnerabilidad como una amenaza prioritaria debido a la existencia de explotación activa confirmada y a la posibilidad de que sea incorporada rápidamente en campañas masivas de ataque dirigidas contra usuarios corporativos, entidades gubernamentales, infraestructura crítica y organizaciones del sector salud.

La disponibilidad pública de información técnica sobre la vulnerabilidad, sumada a la amplia adopción de Chrome en entornos empresariales, incrementa la probabilidad de intentos de explotación oportunistas y dirigidos, especialmente contra organizaciones que mantengan versiones desactualizadas del navegador o que no cuenten con mecanismos efectivos de gestión de vulnerabilidades y actualización de software.

En consecuencia, resulta fundamental que las entidades evalúen de manera inmediata la exposición de sus activos, verifiquen las versiones instaladas de Google Chrome y adopten las medidas de actualización, monitoreo y protección recomendadas por el fabricante para reducir el riesgo de compromiso asociado a esta vulnerabilidad.

### Consecuencias de la explotación

La explotación exitosa de la vulnerabilidad CVE-2026-11645 en Google Chrome podría generar impactos significativos sobre la confidencialidad, integridad y disponibilidad de la



información institucional, especialmente en organizaciones que dependen de aplicaciones web para soportar procesos operativos, administrativos, clínicos y de atención al ciudadano.

Uno de los principales riesgos asociados corresponde al compromiso inicial de estaciones de trabajo mediante la simple interacción del usuario con contenido web malicioso. Debido a que la vulnerabilidad se explota desde el navegador, los atacantes pueden utilizar sitios web comprometidos, campañas de phishing, publicidad maliciosa o enlaces especialmente diseñados para ejecutar código arbitrario sobre los equipos afectados.

En escenarios vulnerables, un atacante podría aprovechar la vulnerabilidad para:

- ejecutar código malicioso dentro del equipo de la víctima;
- comprometer el navegador utilizado por el usuario;
- desplegar herramientas de acceso remoto;
- instalar malware adicional;
- obtener acceso inicial a la red institucional;
- establecer persistencia en el sistema comprometido;
- y preparar el entorno para actividades posteriores de escalamiento de privilegios.

Uno de los impactos más relevantes corresponde a la posible exposición de información sensible almacenada o procesada por el navegador. Actualmente, una gran cantidad de aplicaciones corporativas utilizan sesiones web autenticadas para proporcionar acceso a servicios críticos.

La explotación exitosa podría permitir el acceso no autorizado a:

- cookies de sesión;
- tokens de autenticación;
- credenciales almacenadas;
- formularios completados por los usuarios;
- historiales de navegación;
- información intercambiada con aplicaciones institucionales;



- y datos sensibles visualizados durante la sesión comprometida.

La exposición de estos elementos podría facilitar escenarios de suplantación de identidad digital, secuestro de sesiones y acceso no autorizado a plataformas corporativas.

Otro riesgo significativo corresponde al compromiso de cuentas institucionales utilizadas para acceder a servicios críticos de la organización. Dependiendo del nivel de acceso alcanzado por el atacante, podrían verse comprometidas cuentas relacionadas con:

- correo electrónico institucional;
- directorios corporativos;
- plataformas administrativas;
- sistemas de gestión documental;
- aplicaciones financieras;
- servicios de almacenamiento en la nube;
- plataformas colaborativas;
- y sistemas de autenticación centralizada.

Una vez obtenidas credenciales válidas, los atacantes podrían ampliar progresivamente el alcance del incidente y comprometer activos adicionales dentro de la infraestructura tecnológica.

Las vulnerabilidades de ejecución de código dentro del navegador también representan un riesgo importante debido a su capacidad para facilitar la instalación de malware especializado.

Entre las amenazas que podrían desplegarse posteriormente se encuentran:

- troyanos de acceso remoto;
- spyware;
- infostealers orientados al robo de credenciales;
- ransomware;
- keyloggers;



- herramientas de movimiento lateral;
- malware de espionaje;
- y mecanismos avanzados de persistencia.

La instalación de este tipo de software malicioso puede transformar un incidente inicialmente limitado a una estación de trabajo en una intrusión de mayor alcance dentro de la organización.

Otro aspecto crítico corresponde a la posibilidad de movimiento lateral dentro de la infraestructura institucional. Una vez comprometido el equipo de un usuario, los atacantes podrían intentar identificar activos adicionales conectados a la red corporativa.

Las actividades posteriores podrían incluir:

- reconocimiento interno de la red;
- identificación de servidores críticos;
- enumeración de usuarios privilegiados;
- descubrimiento de servicios corporativos;
- identificación de recursos compartidos;
- búsqueda de credenciales adicionales;
- y acceso progresivo a sistemas de mayor valor para la organización.

La capacidad de movimiento lateral incrementa significativamente el impacto potencial del incidente al permitir que los atacantes extiendan el compromiso más allá del navegador inicialmente afectado.

La explotación de la vulnerabilidad también podría facilitar escenarios de espionaje cibernético orientados a la recopilación de información sensible. Los atacantes podrían monitorear actividades realizadas por los usuarios comprometidos y obtener acceso a información estratégica relacionada con la operación institucional.

Dependiendo del entorno afectado, podrían exponerse:



- documentos institucionales;
- información financiera;
- información contractual;
- planes estratégicos;
- información de proveedores;
- datos de usuarios y clientes;
- información técnica de la infraestructura;
- y documentación interna de seguridad.

La pérdida de confidencialidad de estos activos puede generar consecuencias regulatorias, legales, operacionales y reputacionales para la organización afectada.

En el contexto del sector salud, los riesgos asociados adquieren una relevancia especial debido a la naturaleza sensible de la información procesada por las entidades del sector.

La explotación exitosa podría afectar directamente plataformas utilizadas para:

- consulta de historias clínicas electrónicas;
- gestión de pacientes;
- sistemas de referencia y contrarreferencia;
- servicios de telemedicina;
- plataformas diagnósticas;
- aplicaciones de laboratorio clínico;
- sistemas administrativos hospitalarios;
- y plataformas de interoperabilidad en salud.

El acceso no autorizado a estos entornos podría derivar en la exposición de información clínica protegida y datos personales sujetos a requisitos regulatorios especiales.

Otro impacto relevante corresponde a la posible interrupción de los servicios institucionales. Una vez comprometidos los equipos afectados, los atacantes podrían ejecutar acciones destinadas a degradar o interrumpir la operación normal de los sistemas.



Estas acciones podrían incluir:

- eliminación de archivos críticos;
- modificación de configuraciones;
- sabotaje de aplicaciones;
- cifrado de información mediante ransomware;
- interrupción de servicios tecnológicos;
- bloqueo de cuentas institucionales;
- y afectación de procesos operativos esenciales.

La indisponibilidad de estos servicios puede generar afectaciones directas sobre la continuidad del negocio y la prestación de servicios de salud.

Las organizaciones también podrían enfrentar impactos relacionados con:

- incremento de la superficie de ataque;
- pérdida de visibilidad sobre actividades maliciosas;
- deterioro de la postura de seguridad;
- afectación de procesos de gestión de riesgos;
- aumento de costos asociados a la respuesta al incidente;
- requerimientos regulatorios adicionales;
- y afectaciones reputacionales derivadas de la materialización del incidente.

Adicionalmente, la explotación de esta vulnerabilidad podría ser utilizada como punto de entrada para campañas más amplias orientadas a comprometer la infraestructura tecnológica de la organización.

Entre los escenarios observados habitualmente en este tipo de incidentes se encuentran:

- despliegue de ransomware;
- exfiltración de información sensible;
- robo de credenciales corporativas;



- compromiso de servicios en la nube;
- ataques contra identidades digitales;
- campañas de espionaje dirigidas;
- sabotaje operacional;
- y afectación de procesos críticos de negocio.

El principal riesgo estratégico asociado a esta vulnerabilidad corresponde a que Google Chrome constituye uno de los componentes tecnológicos más utilizados dentro de las organizaciones modernas. Su presencia masiva en estaciones de trabajo administrativas, clínicas y operativas convierte cualquier vulnerabilidad explotada activamente en una amenaza de alto impacto para la seguridad institucional.

La combinación entre explotación activa confirmada, amplia superficie de exposición y capacidad de ejecución de código arbitrario convierte a la vulnerabilidad CVE-2026-11645 en un riesgo prioritario que requiere atención inmediata por parte de las áreas de tecnología, seguridad de la información y ciberseguridad de las entidades del sector salud.

### Modo de explotación del ataque

#### Fase 1 – Identificación de objetivos potenciales

El proceso de explotación inicia cuando los actores de amenaza identifican usuarios u organizaciones que utilizan versiones vulnerables de Google Chrome.

Durante esta etapa, los atacantes realizan actividades orientadas a identificar:

- organizaciones con gran dependencia de aplicaciones web;
- usuarios con acceso a información sensible;
- personal administrativo y directivo;
- funcionarios con acceso privilegiado;
- equipos de tecnología;



- entidades del sector salud;
- y usuarios que utilizan navegadores Chrome desactualizados.

Los actores maliciosos pueden emplear técnicas de reconocimiento abierto (OSINT), recopilación de información pública, monitoreo de redes sociales y análisis de infraestructura expuesta para seleccionar objetivos de interés.

El objetivo principal consiste en identificar usuarios susceptibles de interactuar con contenido malicioso que permita activar la vulnerabilidad.

---

## **Fase 2 – Preparación de la infraestructura maliciosa**

Una vez seleccionados los objetivos, los atacantes preparan los recursos necesarios para ejecutar la explotación.

Durante esta fase podrían desarrollarse actividades relacionadas con:

- creación de sitios web maliciosos;
- compromiso de sitios web legítimos;
- preparación de páginas con código JavaScript especialmente diseñado;
- configuración de servidores de comando y control;
- creación de campañas de phishing;
- generación de enlaces maliciosos;
- y preparación de cargas útiles destinadas a ejecutarse posteriormente sobre los sistemas comprometidos.

El objetivo consiste en disponer de una infraestructura capaz de activar la vulnerabilidad cuando la víctima acceda al contenido preparado por el atacante.

---



### Fase 3 – Distribución del contenido malicioso

Posteriormente, los actores de amenaza buscan que las víctimas accedan al contenido diseñado para explotar la vulnerabilidad.

Las técnicas observadas habitualmente incluyen:

- campañas de phishing por correo electrónico;
- mensajes maliciosos enviados mediante aplicaciones de mensajería;
- enlaces distribuidos a través de redes sociales;
- publicidad maliciosa (Malvertising);
- compromiso de sitios web legítimos;
- ataques de watering hole;
- documentos con enlaces incrustados;
- y redireccionamientos hacia dominios controlados por los atacantes.

En esta etapa, el éxito del ataque depende de que el usuario acceda al contenido especialmente diseñado para activar la vulnerabilidad.

---

### Fase 4 – Activación de la vulnerabilidad en el motor V8

Cuando la víctima accede al sitio web malicioso utilizando una versión vulnerable de Google Chrome, el navegador procesa el contenido JavaScript preparado por el atacante.

Durante esta fase se desencadena la condición de corrupción de memoria asociada a la vulnerabilidad CVE-2026-11645.

La explotación aprovecha errores en el manejo interno de memoria del motor V8 para provocar operaciones de lectura y escritura fuera de los límites permitidos.

Las actividades realizadas por el código malicioso pueden orientarse a:



- manipular estructuras internas de memoria;
- alterar objetos utilizados por el motor JavaScript;
- generar condiciones de corrupción controlada;
- evadir determinadas protecciones de seguridad;
- y preparar la ejecución de código arbitrario dentro del proceso del navegador.

El objetivo consiste en obtener capacidades de ejecución controlada sobre el navegador afectado.

---

### Fase 5 – Ejecución inicial de código malicioso

Una vez explotada exitosamente la vulnerabilidad, el atacante obtiene la capacidad de ejecutar instrucciones dentro del contexto del navegador comprometido.

Dependiendo del escenario de explotación, las actividades iniciales podrían incluir:

- ejecución de código arbitrario;
- descarga de componentes adicionales;
- ejecución de scripts maliciosos;
- establecimiento de comunicaciones externas;
- acceso a recursos locales del navegador;
- manipulación de sesiones activas;
- y preparación de mecanismos de persistencia.

En esta fase se materializa el compromiso inicial del activo afectado.

---

### Fase 6 – Recolección de información sensible

Posteriormente, los atacantes realizan actividades orientadas a identificar y recopilar información de valor almacenada o accesible desde el navegador comprometido.



La información objetivo puede incluir:

- cookies de autenticación;
- tokens de acceso;
- credenciales almacenadas;
- historiales de navegación;
- datos de formularios;
- sesiones activas;
- certificados utilizados por aplicaciones web;
- información de aplicaciones corporativas;
- y datos relacionados con los sistemas utilizados por la organización.

La información obtenida puede ser utilizada para ampliar el alcance del incidente o facilitar compromisos posteriores.

---

### **Fase 7 – Escalamiento de privilegios y compromiso del equipo**

Una vez consolidado el acceso inicial, los atacantes podrían intentar ampliar sus capacidades dentro del sistema comprometido.

Las actividades realizadas pueden incluir:

- ejecución de malware adicional;
- instalación de herramientas de acceso remoto;
- obtención de privilegios elevados;
- evasión de controles de seguridad;
- desactivación de mecanismos de protección;
- explotación de vulnerabilidades adicionales;
- y acceso a recursos restringidos del sistema operativo.



El objetivo consiste en transformar el compromiso del navegador en un compromiso completo de la estación de trabajo.

---

### **Fase 8 – Movimiento lateral dentro de la infraestructura**

Posteriormente, los atacantes pueden intentar expandir el compromiso hacia otros sistemas de la organización.

Las actividades observadas habitualmente incluyen:

- reconocimiento interno de la red;
- identificación de servidores críticos;
- búsqueda de recursos compartidos;
- descubrimiento de servicios corporativos;
- identificación de usuarios privilegiados;
- reutilización de credenciales obtenidas;
- acceso a plataformas corporativas;
- y compromiso progresivo de activos adicionales.

En organizaciones con entornos altamente conectados, esta fase puede facilitar compromisos de mayor alcance sobre la infraestructura tecnológica.

---

### **Fase 9 – Persistencia y control del entorno comprometido**

Una vez alcanzado un nivel suficiente de acceso, los atacantes pueden implementar mecanismos destinados a mantener el control sobre los sistemas comprometidos.

Entre las actividades más comunes se encuentran:

- instalación de puertas traseras (Backdoors);
- creación de cuentas ocultas;
- incorporación de credenciales adicionales;



- modificación de configuraciones de seguridad;
- establecimiento de tareas programadas;
- alteración de mecanismos de monitoreo;
- manipulación de registros de auditoría;
- y creación de canales persistentes de comunicación con infraestructura externa.

El objetivo consiste en garantizar acceso continuo incluso después de que la organización implemente acciones iniciales de contención.

---

### **Fase 10 – Materialización del impacto operacional**

Finalmente, los atacantes pueden utilizar el acceso obtenido para ejecutar acciones orientadas a alcanzar sus objetivos finales.

Dependiendo de la motivación del actor de amenaza, podrían desarrollarse actividades relacionadas con:

- exfiltración de información sensible;
- robo de credenciales corporativas;
- espionaje cibernético;
- secuestro de sesiones institucionales;
- compromiso de aplicaciones críticas;
- despliegue de ransomware;
- sabotaje operacional;
- afectación de servicios tecnológicos;
- compromiso de plataformas clínicas;
- y afectación de la continuidad del negocio.

En el contexto del sector salud, una explotación exitosa podría impactar directamente sistemas clínicos, plataformas administrativas, servicios de interoperabilidad, telemedicina y demás servicios críticos utilizados para soportar la atención de pacientes y la operación institucional.



## Vulnerabilidades asociadas



### Ejecución de código arbitrario mediante corrupción de memoria en el motor V8 (CVE-2026-11645)

- **Descripción:** La vulnerabilidad CVE-2026-11645 corresponde a una falla de tipo Out-of-Bounds Read/Write identificada en el motor V8 de Google Chrome, componente responsable de la ejecución de código JavaScript y WebAssembly dentro del navegador. La debilidad permite que un atacante manipule estructuras de memoria fuera de los límites previstos por la aplicación, generando condiciones que pueden conducir a la ejecución de código arbitrario dentro del contexto del navegador afectado.
- **Impacto:** La explotación exitosa podría permitir que actores maliciosos ejecuten instrucciones controladas dentro del navegador de la víctima, comprometan la integridad del sistema afectado, descarguen malware adicional, obtengan acceso a información sensible y establezcan mecanismos de persistencia. Debido a la explotación activa confirmada por Google, esta vulnerabilidad representa un riesgo significativo para organizaciones que utilicen versiones vulnerables de Chrome.

---

### Compromiso de sesiones autenticadas y robo de credenciales

- **Descripción:** Como consecuencia de la explotación de la vulnerabilidad CVE-2026-11645, los atacantes podrían acceder a información sensible procesada por el navegador durante la sesión del usuario. Esto incluye cookies, tokens de autenticación, credenciales almacenadas y otros elementos utilizados para mantener sesiones activas en aplicaciones corporativas.
- **Impacto:** La exposición de estos elementos podría facilitar el secuestro de sesiones autenticadas, la suplantación de usuarios legítimos, el acceso no autorizado a



aplicaciones institucionales y el compromiso de servicios corporativos críticos. En entornos donde se utilizan mecanismos de autenticación federada o inicio de sesión único (SSO), el impacto potencial podría extenderse a múltiples sistemas simultáneamente.

---

### Instalación de malware posterior a la explotación

- **Descripción:** Una vez obtenida la capacidad de ejecutar código arbitrario dentro del navegador, los atacantes pueden desplegar cargas útiles adicionales orientadas a ampliar el alcance del compromiso. Estas cargas pueden incluir malware especializado diseñado para mantener acceso persistente o facilitar actividades posteriores de espionaje y robo de información.
  - **Impacto:** Los equipos comprometidos podrían ser utilizados para instalar troyanos de acceso remoto, herramientas de espionaje, infostealers, ransomware, keyloggers y otros componentes maliciosos. La instalación de este tipo de software incrementa significativamente la gravedad del incidente y puede derivar en compromisos de mayor alcance dentro de la infraestructura institucional.
- 

### Riesgo de movimiento lateral dentro de la red corporativa

- **Descripción:** Una vez comprometida una estación de trabajo mediante la explotación de la vulnerabilidad, los atacantes podrían utilizar el acceso obtenido para identificar otros activos conectados a la red institucional y expandir progresivamente el alcance del incidente.
- **Impacto:** El movimiento lateral podría permitir el acceso a servidores críticos, servicios de autenticación, plataformas corporativas, sistemas de almacenamiento y otros recursos estratégicos. Este escenario incrementa considerablemente el riesgo de compromisos generalizados sobre la infraestructura tecnológica de la organización.



---

### Exposición de información institucional sensible

- **Descripción:** La explotación de la vulnerabilidad puede facilitar el acceso a información visualizada o procesada por el navegador durante las actividades habituales de los usuarios. Dependiendo de los sistemas utilizados, los atacantes podrían acceder a información corporativa, administrativa o clínica.
- **Impacto:** La exposición de información sensible puede derivar en incidentes relacionados con pérdida de confidencialidad, incumplimientos regulatorios, afectaciones reputacionales y posibles sanciones derivadas de la divulgación no autorizada de datos institucionales o personales.

---

### Riesgo de compromiso de plataformas clínicas y administrativas

- **Descripción:** Las organizaciones del sector salud utilizan ampliamente aplicaciones web para soportar procesos clínicos, administrativos y operacionales. La explotación de la vulnerabilidad podría proporcionar acceso inicial a usuarios con privilegios sobre estos sistemas.
  - **Impacto:** Dependiendo del alcance del compromiso, podrían verse afectados sistemas de historia clínica electrónica, plataformas de laboratorio, servicios de telemedicina, aplicaciones de interoperabilidad, sistemas administrativos hospitalarios y otros servicios críticos para la atención de pacientes y la operación institucional.
- 



## Persistencia y mantenimiento de acceso no autorizado

**Descripción:** Tras comprometer una estación de trabajo, los atacantes pueden implementar mecanismos orientados a mantener acceso prolongado al entorno afectado, incluso después de que la vulnerabilidad inicial haya sido corregida.

**Impacto:** La persistencia dentro de la infraestructura puede facilitar actividades continuas de espionaje, robo de información, movimiento lateral y preparación de ataques posteriores, dificultando los procesos de detección, contención y erradicación del incidente.

---

## Riesgo de campañas dirigidas y explotación masiva

- **Descripción:** Debido a la amplia adopción de Google Chrome en entornos corporativos y personales, las vulnerabilidades explotadas activamente suelen ser incorporadas rápidamente en herramientas automatizadas, kits de explotación y campañas maliciosas distribuidas a gran escala.
- **Impacto:** Las organizaciones que no implementen oportunamente las actualizaciones de seguridad podrían convertirse en objetivos de campañas masivas de compromiso, ataques dirigidos, operaciones de espionaje cibernético, distribución de ransomware y otras actividades maliciosas orientadas a afectar la continuidad operacional y la seguridad de la información institucional.

## Recomendaciones

---

Con el fin de reducir el riesgo asociado a la explotación de la vulnerabilidad CVE-2026-11645 y fortalecer la postura de seguridad de las organizaciones del sector salud, se recomienda implementar las siguientes medidas de prevención, detección, contención y mitigación:

---



## Actualizar inmediatamente Google Chrome

Las organizaciones deben verificar las versiones instaladas de Google Chrome en todos los equipos institucionales y aplicar de manera prioritaria las actualizaciones de seguridad publicadas por Google.

Se recomienda confirmar que los navegadores se encuentren ejecutando las versiones corregidas distribuidas por el fabricante o versiones posteriores.

La actualización debe incluir:

- estaciones de trabajo administrativas;
- equipos clínicos;
- terminales de atención al usuario;
- equipos de teletrabajo;
- dispositivos utilizados por terceros;
- equipos de contratistas;
- y cualquier activo institucional que utilice Google Chrome o navegadores basados en Chromium.

---

## Verificar el estado de actualización de navegadores basados en Chromium

Debido a que múltiples navegadores utilizan componentes derivados del proyecto Chromium, las organizaciones deben validar si otros navegadores implementados en sus entornos también requieren actualizaciones de seguridad.

Se recomienda revisar especialmente:

- Microsoft Edge;
- Brave;
- Opera;



- Vivaldi;
  - y demás navegadores basados en Chromium utilizados dentro de la organización.
- 

### **Fortalecer la gestión de vulnerabilidades**

Las áreas de tecnología y seguridad de la información deben incorporar esta vulnerabilidad dentro de los procesos de gestión de vulnerabilidades institucionales.

Las actividades recomendadas incluyen:

- identificación de activos afectados;
  - priorización de la remediación;
  - verificación de cumplimiento de actualizaciones;
  - monitoreo del estado de mitigación;
  - validación de excepciones autorizadas;
  - y seguimiento de activos que no puedan actualizarse de forma inmediata.
- 

### **Reforzar los controles de navegación segura**

Se recomienda implementar mecanismos de protección destinados a reducir la exposición de los usuarios frente a sitios web maliciosos.

Entre las medidas recomendadas se encuentran:

- filtrado web corporativo;
- inspección de tráfico HTTP y HTTPS;
- bloqueo de dominios maliciosos;
- categorización de contenido web;
- protección DNS;
- análisis de reputación de sitios web;



- y monitoreo de conexiones hacia dominios sospechosos.
- 

### **Fortalecer la protección de estaciones de trabajo**

Las organizaciones deben garantizar que los equipos utilizados por funcionarios y contratistas cuenten con mecanismos adecuados de protección.

Se recomienda verificar:

- soluciones EDR o XDR activas;
  - herramientas antimalware actualizadas;
  - monitoreo de comportamiento anómalo;
  - protección contra explotación de vulnerabilidades;
  - capacidades de aislamiento de equipos comprometidos;
  - monitoreo de procesos sospechosos;
  - y mecanismos de respuesta automatizada.
- 

### **Incrementar el monitoreo de eventos de seguridad**

Las áreas de ciberseguridad deben incrementar temporalmente las actividades de monitoreo sobre eventos relacionados con navegadores web y estaciones de trabajo.

Se recomienda prestar especial atención a:

- ejecuciones anómalas de procesos derivados del navegador;
- conexiones de red inusuales;
- descargas sospechosas;
- creación de procesos secundarios por parte de Chrome;
- actividad relacionada con malware;
- comportamientos asociados a explotación de memoria;



- y comunicaciones hacia infraestructura potencialmente maliciosa.
- 

### Revisar indicadores de compromiso

Las organizaciones deben realizar actividades de búsqueda proactiva de amenazas orientadas a identificar evidencia de explotación previa.

Las revisiones deberían incluir:

- registros de eventos de seguridad;
  - herramientas EDR y XDR;
  - registros de navegación;
  - sistemas de monitoreo de red;
  - servidores proxy;
  - plataformas SIEM;
  - y demás fuentes relevantes de telemetría institucional.
- 

### Aplicar el principio de mínimo privilegio

Se recomienda limitar los privilegios de los usuarios finales para reducir el impacto potencial derivado de la explotación de vulnerabilidades en estaciones de trabajo.

Las organizaciones deberían:

- restringir privilegios administrativos locales;
  - controlar la instalación de software;
  - limitar el acceso a recursos críticos;
  - implementar controles de elevación de privilegios;
  - y monitorear el uso de cuentas privilegiadas.
- 



### **Fortalecer los mecanismos de autenticación**

Con el fin de reducir el impacto asociado al robo de credenciales y secuestro de sesiones, se recomienda fortalecer los mecanismos de autenticación utilizados por la organización.

Las medidas recomendadas incluyen:

- autenticación multifactor (MFA);
  - gestión segura de contraseñas;
  - autenticación basada en riesgo;
  - monitoreo de accesos anómalos;
  - protección de identidades privilegiadas;
  - revisión periódica de cuentas;
  - y revocación inmediata de accesos innecesarios.
- 

### **Sensibilizar a los usuarios institucionales**

Las campañas de explotación suelen apoyarse en técnicas de ingeniería social para dirigir a las víctimas hacia contenido malicioso.

Por esta razón se recomienda reforzar las actividades de concienciación sobre:

- phishing;
  - enlaces sospechosos;
  - descargas no autorizadas;
  - navegación segura;
  - protección de credenciales;
  - reporte de incidentes;
  - y buenas prácticas de ciberseguridad.
- 



### **Fortalecer la capacidad de respuesta ante incidentes**

Las entidades deben verificar que sus procedimientos de respuesta a incidentes contemplen escenarios relacionados con la explotación de vulnerabilidades en navegadores web.

Se recomienda validar:

- procedimientos de identificación;
- mecanismos de contención;
- capacidades de análisis forense;
- procedimientos de recuperación;
- procesos de comunicación interna;
- gestión de evidencias;
- y actividades de lecciones aprendidas.

---

### **Recomendaciones específicas para el sector salud**

Las instituciones prestadoras de servicios de salud, entidades administradoras, operadores tecnológicos y demás organizaciones del sector deberán priorizar la actualización de equipos que tengan acceso a:

- historias clínicas electrónicas;
- plataformas de interoperabilidad;
- sistemas de información hospitalaria;
- aplicaciones de laboratorio clínico;
- servicios de telemedicina;
- sistemas diagnósticos;
- plataformas administrativas;
- y demás servicios críticos relacionados con la atención de pacientes.



La explotación activa confirmada de esta vulnerabilidad, sumada a la amplia adopción de Google Chrome dentro de los entornos corporativos, convierte la actualización inmediata de los sistemas afectados en la medida de mitigación más efectiva para reducir el riesgo de compromiso institucional.

## Conclusiones



La vulnerabilidad CVE-2026-11645 representa una amenaza significativa para las organizaciones debido a su capacidad para permitir la ejecución de código arbitrario mediante la explotación de una falla de corrupción de memoria en el motor V8 de Google Chrome. La confirmación de explotación activa por parte de Google incrementa considerablemente el nivel de riesgo, ya que evidencia la existencia de actores de amenaza que están aprovechando esta vulnerabilidad en escenarios reales.

La amplia adopción de Google Chrome en entornos corporativos convierte esta vulnerabilidad en un vector de ataque de alto impacto. Las estaciones de trabajo utilizadas para acceder a aplicaciones institucionales, servicios en la nube, plataformas administrativas y sistemas críticos pueden convertirse en puntos de entrada para comprometer la infraestructura tecnológica de una organización.

Uno de los aspectos más relevantes de este escenario es que la explotación puede producirse a través de actividades cotidianas de navegación web. La simple interacción de un usuario con contenido malicioso, sitios web comprometidos o enlaces distribuidos mediante campañas de ingeniería social podría facilitar el compromiso inicial de los sistemas afectados.

Las organizaciones deben considerar que la explotación exitosa no se limita al navegador comprometido. Una vez obtenido acceso inicial, los atacantes podrían desplegar malware adicional, realizar movimientos laterales, obtener credenciales, comprometer identidades digitales y ampliar progresivamente el alcance del incidente dentro de la infraestructura institucional.



En el sector salud, el riesgo adquiere una importancia especial debido a la creciente dependencia de plataformas web utilizadas para soportar procesos asistenciales, administrativos y operacionales. La afectación de estaciones de trabajo con acceso a historias clínicas electrónicas, plataformas hospitalarias, servicios de interoperabilidad, sistemas diagnósticos y herramientas de telemedicina podría generar impactos significativos sobre la prestación de servicios y la continuidad operativa.

La exposición potencial de información sensible, credenciales institucionales y datos relacionados con pacientes incrementa los riesgos asociados a la confidencialidad de la información, así como las posibles implicaciones regulatorias, legales y reputacionales derivadas de un incidente de seguridad.

Las entidades deben priorizar la identificación de activos afectados, la aplicación inmediata de las actualizaciones de seguridad publicadas por Google y el fortalecimiento de sus capacidades de monitoreo, detección y respuesta ante incidentes. La gestión oportuna de esta vulnerabilidad constituye una medida esencial para reducir la superficie de ataque y limitar las oportunidades de explotación por parte de actores maliciosos.

Finalmente, se recomienda a todas las organizaciones del ecosistema digital de salud mantener una vigilancia permanente sobre nuevas actualizaciones de seguridad relacionadas con navegadores web, fortalecer los procesos de gestión de vulnerabilidades y promover una cultura de ciberseguridad que permita responder de manera efectiva frente a amenazas emergentes que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional.

#### Fuentes:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk>
- [https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop\\_0153744567.html](https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html)



- <https://chromereleases.googleblog.com>
- <https://nvd.nist.gov>
- <https://www.cve.org>
- <https://security.googleblog.com>
- <https://chromium.org>
- <https://securityonline.info/chrome-security-update/>
- <https://www.bleepingcomputer.com/news/security/google-patches-fifth-chrome-zero-day-bug-exploited-in-attacks-this-year/>
- <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- <https://attack.mitre.org>
- <https://www.cve.org>
- <https://nvd.nist.gov>
- <https://support.google.com/chrome/a>
- [https://www.cisecurity.org/benchmark/google\\_chrome](https://www.cisecurity.org/benchmark/google_chrome)
- <https://owasp.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) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.

