

Alerta ID:	56
Fecha del reporte:	23/07/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidad crítica en la extensión Adobe Acrobat para Google Chrome
Herramienta de detección	N/A
Activos involucrados:	Estaciones de trabajo que ejecuten Google Chrome o navegadores basados en Chromium con la extensión Adobe Acrobat instalada; equipos administrativos y asistenciales utilizados para acceder a aplicaciones clínicas; plataformas de Historia Clínica Electrónica (HCE); sistemas PACS; aplicaciones de laboratorio; plataformas de telemedicina; portales institucionales; correo electrónico corporativo; aplicaciones SaaS; servicios web autenticados; plataformas documentales; equipos utilizados por personal clínico y administrativo; así como cualquier activo tecnológico que utilice navegadores web para acceder a información institucional o procesar datos sensibles del sector salud.
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la vulnerabilidad **CVE-2026-48294**, identificada en la extensión **Adobe Acrobat PDF Extension para Google Chrome**, la cual podría ser explotada mediante una técnica de **Universal Cross-Site Scripting (UXSS)** para acceder a información procesada por aplicaciones web autenticadas y comprometer la confidencialidad de los datos institucionales.

La vulnerabilidad afecta un componente ampliamente utilizado en entornos empresariales y puede ser aprovechada para eludir parcialmente los mecanismos de aislamiento del navegador, facilitando el acceso no autorizado a información visualizada por el usuario durante sus sesiones de navegación. Debido al uso intensivo de aplicaciones web para soportar procesos clínicos, administrativos y asistenciales, las organizaciones del sector salud podrían

Alerta Vulnerabilidad extensión Adobe Acrobat para Google



CSIRTSALUD-AV-20260723-56

TLP: CLEAR

verse expuestas a la divulgación de información sensible si no implementan oportunamente las actualizaciones de seguridad publicadas por Adobe.

El propósito de esta alerta es proporcionar a las entidades del sector salud información técnica que facilite la identificación de los activos potencialmente afectados, la validación de las versiones instaladas, la aplicación prioritaria de las actualizaciones de seguridad y la implementación de medidas de prevención, monitoreo y respuesta que reduzcan el riesgo de explotación y fortalezcan la protección de la información institucional.

Descripción:

Investigadores de **Guardio Labs** identificaron la vulnerabilidad **CVE-2026-48294**, denominada **HermeticReader**, que afecta la extensión oficial **Adobe Acrobat PDF Extension** para Google Chrome. La falla corresponde a un escenario de **Universal Cross-Site Scripting (UXSS)** que permite abusar de los privilegios de la extensión para acceder a información procesada por aplicaciones web autenticadas, vulnerando parcialmente los mecanismos de aislamiento implementados por el navegador.

La investigación demuestra que un atacante puede construir una cadena de explotación utilizando la interacción entre la extensión y el navegador para acceder a información que normalmente estaría protegida por la **Same-Origin Policy (SOP)**. La explotación puede iniciarse cuando la víctima visita un sitio web especialmente diseñado, sin requerir la instalación de malware ni el compromiso previo de la aplicación web objetivo.

Aunque la prueba de concepto fue realizada utilizando **WhatsApp Web**, el riesgo no se limita a esta plataforma. Cualquier aplicación web que procese información sensible dentro del navegador podría verse expuesta si se cumplen las condiciones necesarias para la explotación. En el sector salud, este escenario representa un riesgo para plataformas de Historia Clínica Electrónica (HCE), sistemas hospitalarios, aplicaciones de laboratorio, portales administrativos y demás servicios web utilizados diariamente por el personal asistencial y administrativo.

La amplia distribución de la extensión Adobe Acrobat y el uso permanente de aplicaciones web en las organizaciones incrementan la superficie de ataque y convierten esta vulnerabilidad en un riesgo significativo para la confidencialidad de la información. Por ello, resulta prioritario identificar los equipos afectados, verificar las versiones instaladas, aplicar las actualizaciones



de seguridad publicadas por Adobe y fortalecer el monitoreo de las extensiones autorizadas dentro de los navegadores corporativos.

Vulnerabilidad con evidencia de explotación

La presente alerta aborda la vulnerabilidad CVE-2026-48294, identificada en la extensión oficial Adobe Acrobat PDF Extension para Google Chrome. La falla fue descubierta por investigadores de Guardio Labs, quienes demostraron que un atacante puede aprovechar una debilidad en el manejo de contenido web por parte de la extensión para ejecutar un ataque de Universal Cross-Site Scripting (UXSS) y acceder a información procesada por aplicaciones web autenticadas.

CVE-2026-48294 – Adobe Acrobat PDF Extension

- **Descripción:** La vulnerabilidad corresponde a un escenario de Universal Cross-Site Scripting (UXSS) originado por un manejo inadecuado de los privilegios otorgados a la extensión Adobe Acrobat dentro del navegador Google Chrome. Un sitio web especialmente diseñado puede inducir a la extensión a realizar operaciones sobre contenido perteneciente a otros dominios, permitiendo acceder a información que normalmente estaría protegida por los mecanismos de aislamiento implementados por el navegador.
- **Impacto:** La explotación exitosa puede permitir la divulgación de información sensible procesada por aplicaciones web autenticadas, incluyendo contenido visualizado por el usuario durante su sesión de navegación. Dependiendo del contexto de uso, un actor de amenaza podría acceder a información confidencial, obtener datos utilizados durante procesos administrativos o clínicos y facilitar actividades posteriores de reconocimiento, espionaje o robo de información.
- **Estado de explotación:** Al momento de la emisión de esta alerta no existe evidencia pública de explotación masiva de la vulnerabilidad en entornos reales. No obstante, los investigadores publicaron una prueba de concepto funcional que demuestra la viabilidad técnica del ataque, razón por la cual se recomienda priorizar la actualización de la extensión en todos los activos afectados.

Análisis técnico de la vulnerabilidad

La vulnerabilidad se origina en la forma como la extensión Adobe Acrobat interactúa con el navegador para ofrecer funcionalidades relacionadas con la visualización y administración de documentos PDF. Debido a los permisos otorgados por Chromium, la extensión dispone de capacidades superiores a las disponibles para un sitio web convencional, lo que incrementa el impacto potencial de cualquier error presente en su implementación.

Los investigadores demostraron que un atacante puede aprovechar dichas capacidades para ejecutar una cadena de acciones que termina accediendo a contenido perteneciente a otros orígenes. Este comportamiento rompe parcialmente el modelo de seguridad basado en la Same-Origin Policy (SOP), mecanismo diseñado para impedir que un sitio web interactúe con información perteneciente a dominios diferentes.

La investigación evidencia que la explotación puede realizarse sin comprometer directamente la aplicación web objetivo. En lugar de atacar el servidor o vulnerar el proceso de autenticación, el atacante utiliza una página especialmente diseñada para abusar del comportamiento de la extensión instalada localmente en el equipo de la víctima. Esta característica reduce considerablemente la complejidad del ataque y dificulta su identificación mediante controles tradicionales de seguridad perimetral.

Durante la prueba de concepto publicada por los investigadores, la vulnerabilidad fue utilizada para acceder a información presentada en WhatsApp Web, demostrando que una extensión con privilegios elevados puede convertirse en un punto de exposición para aplicaciones web autenticadas. Aunque la demostración se realizó sobre esta plataforma, el riesgo puede extenderse a otros servicios que procesen información sensible dentro del navegador.

En organizaciones del sector salud, donde gran parte de la operación diaria depende de aplicaciones web utilizadas desde estaciones de trabajo corporativas, la explotación de esta vulnerabilidad podría facilitar el acceso a información administrativa o clínica procesada durante sesiones autenticadas, incrementando el riesgo de fuga de información y afectando la confidencialidad de los datos institucionales.

La disponibilidad pública de información técnica sobre la vulnerabilidad incrementa la probabilidad de que actores maliciosos desarrollen nuevas variantes de explotación o integren esta técnica en campañas de phishing y sitios web comprometidos dirigidos contra

organizaciones que aún mantengan versiones vulnerables de la extensión Adobe Acrobat. Por esta razón, resulta recomendable que las entidades del sector salud prioricen la actualización de los equipos afectados y fortalezcan el monitoreo de las extensiones instaladas en los navegadores corporativos.

Productos y versiones afectadas

La vulnerabilidad **CVE-2026-48294** afecta la **Adobe Acrobat PDF Extension** para navegadores basados en Chromium. Debido a que esta extensión es ampliamente utilizada para visualizar, convertir, firmar y administrar documentos PDF desde el navegador, su presencia es común en estaciones de trabajo corporativas, equipos administrativos y dispositivos utilizados para acceder a aplicaciones institucionales.

Las entidades del sector salud deben identificar los equipos donde la extensión se encuentre instalada, verificar la versión actualmente implementada y validar que se haya aplicado la actualización de seguridad publicada por Adobe. La identificación temprana de las versiones vulnerables constituye una actividad prioritaria dentro de los procesos de gestión de vulnerabilidades y administración de activos tecnológicos.

Adobe Acrobat PDF Extension

Las versiones vulnerables corresponden a:

- Adobe Acrobat PDF Extension para Google Chrome **26.5.2.2 y versiones anteriores**.

La vulnerabilidad fue corregida por Adobe en las versiones posteriores publicadas a través de la Chrome Web Store, por lo que se recomienda verificar que la actualización haya sido instalada correctamente en todos los equipos administrados.

Navegadores afectados

La vulnerabilidad impacta la extensión cuando es utilizada en navegadores compatibles con el modelo de extensiones de Chromium, entre ellos:

- Google Chrome.
- Microsoft Edge (Chromium), cuando la extensión se encuentre instalada.
- Otros navegadores basados en Chromium que permitan la instalación de la extensión Adobe Acrobat.

Aunque la vulnerabilidad reside en la extensión y no en el navegador, cualquier equipo que ejecute una versión vulnerable del complemento podría encontrarse expuesto.

Activos con mayor nivel de exposición

Las organizaciones del sector salud deberán priorizar la revisión de los siguientes activos:

- Estaciones de trabajo utilizadas por personal médico y asistencial.
- Equipos administrativos que procesen documentos institucionales.
- Equipos utilizados para acceder a plataformas de Historia Clínica Electrónica (HCE).
- Sistemas empleados para la gestión documental y firma electrónica.
- Equipos utilizados para acceder a aplicaciones financieras, administrativas y de contratación.
- Equipos con acceso a información clínica, datos personales o información financiera.

Especial atención debe prestarse a los equipos compartidos, estaciones de trabajo ubicadas en áreas asistenciales y dispositivos utilizados por usuarios con privilegios elevados, debido al mayor volumen de información sensible procesada durante sus sesiones de navegación.

Las entidades que administren sus navegadores mediante políticas corporativas deberán validar que la actualización de la extensión se haya distribuido correctamente a todos los usuarios y confirmar que no permanezcan versiones vulnerables instaladas en equipos fuera de los mecanismos de administración centralizada.

Consideraciones para el sector salud

La utilización de navegadores web como plataforma principal para acceder a aplicaciones clínicas y administrativas incrementa la importancia de mantener un control permanente sobre las extensiones autorizadas dentro de la organización. A diferencia de otras vulnerabilidades que afectan únicamente a una aplicación específica, **CVE-2026-48294** puede impactar

Alerta Vulnerabilidad extensión Adobe Acrobat para Google



CSIRTSALUD-AV-20260723-56

TLP: CLEAR

múltiples servicios web utilizados diariamente por el personal institucional, independientemente del fabricante de dichas aplicaciones.

En muchas entidades del sector salud, los navegadores son utilizados de manera simultánea para consultar historias clínicas, revisar resultados de laboratorio, acceder a sistemas PACS, gestionar procesos administrativos, consultar plataformas gubernamentales y utilizar servicios de correo electrónico y colaboración. La coexistencia de estas aplicaciones dentro de una misma sesión de navegación incrementa el impacto potencial de una vulnerabilidad que permita acceder a información presentada por diferentes servicios web autenticados.

Por esta razón, la gestión de extensiones de navegador debe formar parte de los procesos institucionales de endurecimiento de estaciones de trabajo, administración de activos y gestión de vulnerabilidades. Las organizaciones deberían mantener un inventario actualizado de las extensiones autorizadas, restringir la instalación de complementos no aprobados y verificar periódicamente que las actualizaciones de seguridad se apliquen de forma oportuna mediante herramientas de administración centralizada.

La identificación temprana de equipos con versiones vulnerables, junto con la implementación de políticas para controlar las extensiones permitidas, constituye una medida efectiva para reducir la superficie de ataque y fortalecer la seguridad de los navegadores utilizados para soportar los procesos misionales del sector salud.

Consecuencias de la Explotación

La explotación exitosa de la vulnerabilidad **CVE-2026-48294** puede comprometer la confidencialidad de la información procesada mediante aplicaciones web autenticadas, permitiendo que un actor de amenaza obtenga acceso no autorizado a datos visualizados por el usuario durante su sesión de navegación. Debido a que la vulnerabilidad reside en una extensión ampliamente utilizada para la gestión de documentos PDF, el riesgo no se limita a una aplicación específica, sino que puede afectar múltiples servicios web utilizados de forma simultánea dentro del navegador.

En las organizaciones del sector salud, donde gran parte de los procesos clínicos, administrativos y operacionales dependen de plataformas web, la explotación de esta vulnerabilidad podría facilitar la exposición de información clínica, datos personales, documentos institucionales y otra información sensible procesada durante la jornada laboral.



Alerta Vulnerabilidad extensión Adobe Acrobat para Google



CSIRTSALUD-AV-20260723-56

TLP: CLEAR

Aunque la vulnerabilidad no compromete directamente los servidores institucionales, la información obtenida desde las estaciones de trabajo puede ser utilizada para apoyar fases posteriores de un ataque dirigido.

Uno de los principales riesgos corresponde a la divulgación no autorizada de información presentada en aplicaciones web autenticadas. Dependiendo de los privilegios del usuario afectado, un atacante podría obtener acceso a datos relacionados con pacientes, procesos administrativos, documentos institucionales, plataformas financieras, sistemas documentales o aplicaciones de soporte utilizadas por la organización.

La información obtenida durante la explotación también puede facilitar actividades de reconocimiento sobre la infraestructura tecnológica. El conocimiento de nombres de usuarios, estructuras organizacionales, aplicaciones utilizadas, procedimientos internos o información operativa puede ser empleado para preparar campañas de ingeniería social, phishing dirigido o ataques posteriores con un mayor nivel de efectividad.

En organizaciones que utilizan plataformas de mensajería web para actividades institucionales, la vulnerabilidad podría permitir el acceso a conversaciones visibles, nombres de contactos u otra información presentada durante la sesión del usuario. Este tipo de información puede contener instrucciones operativas, datos de pacientes, información administrativa o referencias a procesos internos cuya divulgación afectaría la confidencialidad institucional.

Desde la perspectiva del cumplimiento normativo, la exposición de información personal o datos relacionados con la salud puede generar incidentes asociados al tratamiento de datos personales y al incumplimiento de las obligaciones de confidencialidad establecidas por la normativa colombiana. La divulgación no autorizada de esta información podría afectar la confianza de los usuarios, generar impactos reputacionales y dar lugar a procesos de investigación por parte de las autoridades competentes.

Aunque la vulnerabilidad no fue diseñada para ejecutar código remoto sobre el sistema operativo, la información obtenida mediante su explotación puede servir como punto de partida para ataques más complejos. Un actor de amenaza podría utilizar los datos recopilados para identificar usuarios con privilegios elevados, reconocer aplicaciones críticas, obtener información de autenticación visible durante la navegación o planificar nuevas acciones dirigidas contra la organización.



Alerta Vulnerabilidad extensión Adobe Acrobat para Google



CSIRTSALUD-AV-20260723-56

TLP: CLEAR

Las organizaciones que mantengan versiones vulnerables de la extensión Adobe Acrobat deben considerar este riesgo dentro de sus procesos de gestión de vulnerabilidades, especialmente cuando los equipos afectados tengan acceso a información clínica, administrativa o financiera, o sean utilizados por personal con responsabilidades críticas dentro de la operación institucional.

En términos generales, la explotación de esta vulnerabilidad podría permitir a un actor de amenaza:

- Obtener acceso no autorizado a información presentada por aplicaciones web autenticadas.
- Exponer información clínica, administrativa, financiera o documental procesada durante la navegación.
- Obtener información utilizada para actividades de reconocimiento sobre la organización.
- Identificar usuarios, contactos, procedimientos internos y aplicaciones institucionales.
- Facilitar campañas posteriores de phishing dirigido, ingeniería social o espionaje.
- Comprometer la confidencialidad de información relacionada con pacientes y procesos asistenciales.
- Incrementar el riesgo de fuga de información sensible y afectaciones reputacionales para la organización.

Las entidades del sector salud que utilicen la extensión Adobe Acrobat en estaciones de trabajo corporativas deben priorizar la aplicación de las actualizaciones de seguridad publicadas por Adobe, verificar la correcta distribución de las versiones corregidas y fortalecer los controles de seguridad asociados a la administración de navegadores y extensiones autorizadas. La actualización oportuna, acompañada de actividades de monitoreo y revisión de eventos relacionados con el navegador, constituye la medida más efectiva para reducir la probabilidad de explotación y preservar la confidencialidad de la información institucional.

Indicadores de compromiso (IoC) y actividades de detección

La explotación de la vulnerabilidad CVE-2026-48294 puede generar diversos comportamientos anómalos relacionados con el navegador, las extensiones instaladas y las aplicaciones web utilizadas por el usuario. Debido a que la vulnerabilidad aprovecha los privilegios de la extensión Adobe Acrobat para interactuar con contenido web autenticado, las actividades de monitoreo deben enfocarse en eventos asociados a la ejecución del navegador,



el comportamiento de las extensiones y las comunicaciones establecidas desde las estaciones de trabajo.

Las organizaciones del sector salud deberán fortalecer temporalmente el monitoreo sobre los equipos que tengan instalada la extensión Adobe Acrobat, verificando que las actualizaciones de seguridad hayan sido aplicadas y que no existan evidencias de intentos de explotación o comportamientos anómalos relacionados con la actividad del navegador.

Indicadores de compromiso generales

Durante las actividades de monitoreo e investigación, se recomienda prestar especial atención a los siguientes comportamientos:

- Acceso a sitios web no habituales seguido de interacción con aplicaciones institucionales autenticadas.
- Actividad inusual asociada a la extensión Adobe Acrobat durante sesiones de navegación.
- Solicitudes HTTP o HTTPS generadas desde la extensión hacia recursos diferentes a los esperados para su funcionamiento normal.
- Incremento inesperado de eventos relacionados con extensiones del navegador.
- Acceso simultáneo a múltiples aplicaciones web institucionales desde la misma sesión del navegador inmediatamente después de visitar sitios externos.
- Modificaciones no autorizadas en la configuración o permisos de extensiones instaladas.
- Instalación o actualización de extensiones fuera de los mecanismos corporativos de administración.
- Incremento inusual en el consumo de memoria o procesamiento asociado al navegador durante la visualización de contenido web.

Actividades de detección para Google Chrome y navegadores basados en Chromium

Los navegadores constituyen el principal punto de interacción con la vulnerabilidad. Se recomienda monitorear:

- Instalación, eliminación o actualización no autorizada de extensiones.

Alerta Vulnerabilidad extensión Adobe Acrobat para Google



CSIRTSALUD-AV-20260723-56

TLP: CLEAR

- Cambios en los permisos asignados a la extensión Adobe Acrobat.
- Acceso de la extensión a múltiples dominios durante una misma sesión.
- Ejecución de procesos del navegador con parámetros inusuales.
- Eventos relacionados con la ejecución de extensiones fuera del comportamiento habitual.
- Navegación hacia sitios recientemente registrados o con baja reputación antes de acceder a aplicaciones institucionales.
- Intentos de deshabilitar funciones de seguridad del navegador o modificar políticas corporativas.

Los equipos SOC deberán correlacionar estos eventos con alertas generadas por soluciones EDR/XDR, plataformas SIEM y herramientas de protección de navegación para identificar posibles intentos de explotación.

Actividades de detección para aplicaciones web institucionales

Las aplicaciones utilizadas diariamente por las entidades del sector salud pueden presentar comportamientos que ayuden a identificar actividades sospechosas derivadas de la explotación de esta vulnerabilidad.

Se recomienda revisar:

- Accesos inusuales a aplicaciones web desde estaciones de trabajo previamente identificadas como vulnerables.
- Consultas repetitivas sobre registros clínicos o administrativos sin una justificación operacional.
- Incremento anormal en la visualización de documentos PDF o información histórica.
- Cambios inesperados en los patrones de navegación de usuarios autenticados.
- Consultas consecutivas sobre múltiples registros o expedientes en intervalos reducidos de tiempo.
- Actividades realizadas desde sesiones autenticadas inmediatamente después de acceder a sitios externos no relacionados con la operación institucional.



Actividades de detección para Microsoft Defender, EDR y XDR

Las soluciones de protección de endpoints pueden proporcionar información relevante para identificar actividades asociadas con la explotación de la vulnerabilidad.

Se recomienda monitorear:

- Alertas relacionadas con comportamiento anómalo de Google Chrome o Microsoft Edge.
- Eventos asociados a modificaciones de extensiones del navegador.
- Actividad inusual de procesos derivados del navegador.
- Cambios en directorios donde se almacenan extensiones de Chromium.
- Conexiones establecidas hacia dominios previamente no observados por el activo.
- Alertas relacionadas con comportamiento anómalo del navegador generadas por Microsoft Defender SmartScreen o mecanismos equivalentes.

Actividades de detección mediante SIEM

Los equipos de monitoreo deberán establecer reglas de correlación que permitan identificar eventos relacionados con la vulnerabilidad, incluyendo:

- Equipos que ejecuten versiones vulnerables de la extensión Adobe Acrobat.
- Usuarios que accedan a sitios externos inmediatamente antes de utilizar aplicaciones institucionales críticas.
- Incremento de eventos relacionados con extensiones de navegador.
- Alertas EDR asociadas al navegador correlacionadas con autenticaciones exitosas en aplicaciones institucionales.
- Cambios de versión de la extensión fuera de las ventanas autorizadas de mantenimiento.
- Equipos que permanezcan utilizando versiones vulnerables después de la publicación de la actualización de seguridad.

Recomendaciones para el monitoreo continuo

Mientras las actividades de actualización son ejecutadas, las entidades del sector salud deberán mantener un monitoreo reforzado sobre las estaciones de trabajo que utilicen la extensión Adobe Acrobat, priorizando aquellas con acceso a Historia Clínica Electrónica (HCE),

sistemas hospitalarios, plataformas de laboratorio, aplicaciones financieras y servicios administrativos críticos.

La información recopilada mediante las soluciones SIEM, EDR, XDR y plataformas de administración de navegadores deberá correlacionarse con los inventarios de activos y los procesos de gestión de vulnerabilidades para identificar oportunamente equipos que continúen expuestos y verificar la correcta aplicación de las actualizaciones de seguridad publicadas por Adobe.

Medidas de Prevención



Las entidades del sector salud deberán implementar de manera prioritaria las siguientes medidas para reducir el riesgo de explotación de la vulnerabilidad **CVE-2026-48294** y fortalecer la seguridad de los navegadores utilizados para acceder a información institucional.

- **Actualizar la extensión Adobe Acrobat:** Verificar que la totalidad de los equipos que utilicen la **Adobe Acrobat PDF Extension** ejecuten la versión corregida publicada por Adobe. Las organizaciones que administren navegadores mediante políticas corporativas deberán confirmar que la actualización haya sido distribuida correctamente a todos los usuarios y que no permanezcan versiones vulnerables instaladas.
- **Fortalecer la gestión de extensiones:** Implementar políticas que permitan únicamente la instalación de extensiones previamente autorizadas por la organización. Se recomienda mantener un inventario actualizado de las extensiones instaladas, revisar periódicamente los permisos asignados y eliminar aquellas que no sean necesarias para el desarrollo de las funciones institucionales.
- **Restringir privilegios de instalación:** Limitar la capacidad de los usuarios para instalar o modificar extensiones del navegador sin autorización del área de tecnologías de la información. La administración centralizada reduce significativamente el riesgo asociado a la utilización de complementos vulnerables o no autorizados.
- **Mantener actualizado el navegador:** Aunque la vulnerabilidad reside en la extensión, es recomendable mantener Google Chrome y los demás navegadores basados en

Alerta Vulnerabilidad extensión Adobe Acrobat para Google



CSIRTSALUD-AV-20260723-56

TLP: CLEAR

Chromium permanentemente actualizados, asegurando la instalación oportuna de las actualizaciones de seguridad publicadas por sus fabricantes.

- **Fortalecer la navegación segura:** Promover el acceso únicamente a sitios web confiables y reforzar las campañas institucionales de sensibilización frente a enlaces sospechosos, campañas de phishing y sitios web fraudulentos que puedan ser utilizados para iniciar la cadena de explotación.
- **Aplicar el principio de mínimo privilegio:** Restringir el acceso de los usuarios únicamente a las aplicaciones y recursos necesarios para el cumplimiento de sus funciones. La reducción de privilegios disminuye el impacto potencial en caso de que una estación de trabajo resulte comprometida.
- **Gestionar permanentemente las vulnerabilidades:** Incorporar las extensiones del navegador dentro de los procesos institucionales de gestión de vulnerabilidades, verificando periódicamente la publicación de nuevos boletines

Medidas de detección y mitigación

Además de la aplicación de las actualizaciones de seguridad, las organizaciones deberán fortalecer temporalmente las actividades de monitoreo sobre las estaciones de trabajo que utilicen la extensión Adobe Acrobat, con el propósito de identificar oportunamente posibles intentos de explotación o actividades anómalas relacionadas con el navegador.

Se recomienda verificar periódicamente el inventario de extensiones instaladas, identificar versiones vulnerables, revisar los permisos otorgados a cada complemento y validar que únicamente permanezcan habilitadas las extensiones autorizadas por la organización.

Los equipos responsables del monitoreo de seguridad deberán correlacionar los eventos generados por los navegadores con la información proveniente de soluciones EDR, XDR, SIEM y plataformas de administración de vulnerabilidades, prestando especial atención a cambios inesperados en las extensiones, actividad inusual durante las sesiones de navegación y comportamientos que difieran del perfil habitual de los usuarios.

Las entidades que administren navegadores mediante políticas corporativas deberán validar que las configuraciones de seguridad permanezcan vigentes, restringiendo la instalación de



nuevas extensiones y verificando que los usuarios no puedan modificar los controles establecidos por la organización.

En equipos utilizados para acceder a plataformas de Historia Clínica Electrónica (HCE), sistemas hospitalarios, aplicaciones financieras y demás servicios críticos, se recomienda incrementar temporalmente las actividades de monitoreo hasta confirmar que la totalidad de los activos afectados hayan recibido las actualizaciones correspondientes.

Respuesta ante incidentes

Si una organización identifica evidencias que sugieran la posible explotación de la vulnerabilidad **CVE-2026-48294**, deberá activar su procedimiento institucional de respuesta a incidentes de seguridad de la información e iniciar las actividades de análisis y contención correspondientes.

Como primera medida, se recomienda identificar los equipos potencialmente afectados, verificar la versión instalada de la extensión Adobe Acrobat y confirmar si la actualización de seguridad fue aplicada correctamente. En caso de detectarse versiones vulnerables, estas deberán actualizarse inmediatamente o, cuando sea necesario, deshabilitar temporalmente la extensión hasta completar el proceso de remediación.

Posteriormente, deberá realizarse una revisión de los registros generados por las soluciones EDR, XDR, SIEM y herramientas de administración de navegadores con el fin de identificar comportamientos anómalos asociados a la actividad del navegador, accesos inusuales a aplicaciones web, modificaciones en extensiones o cualquier otra evidencia que permita determinar el alcance del incidente.

Si existe la posibilidad de que información institucional haya sido expuesta, la organización deberá evaluar el impacto sobre los procesos asistenciales, administrativos y operacionales, identificar la información potencialmente comprometida e implementar las medidas de contención necesarias para reducir el riesgo de nuevas afectaciones.

Como parte de las actividades de recuperación, se recomienda verificar la correcta actualización de todos los equipos afectados, revisar las políticas de administración de extensiones, fortalecer los mecanismos de monitoreo continuo y documentar las lecciones aprendidas con el propósito de mejorar los procesos institucionales de gestión de vulnerabilidades y respuesta a incidentes.

Alerta Vulnerabilidad extensión Adobe Acrobat para Google



CSIRTSALUD-AV-20260723-56

TLP: CLEAR

Finalmente, cuando el incidente involucre información personal, datos relacionados con la salud o afecte la prestación de servicios esenciales, la entidad deberá seguir los procedimientos internos de notificación y reporte establecidos por la organización, así como las obligaciones regulatorias aplicables.

Fuentes:

- <https://thehackernews.com/2026/07/adobe-acrobat-extension-flaw-let.html>
- <https://guard.io/labs/hermeticreader>
- <https://helpx.adobe.com/security/products/acrobat/apsb26-95.html>
- <https://nvd.nist.gov/vuln/detail/CVE-2026-48294>
- <https://www.cve.org/CVERecord?id=CVE-2026-48294>
- <https://developer.chrome.com/docs/extensions>
- <https://developer.chrome.com/docs/extensions/develop/security-privacy>
- https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy
- <https://owasp.org/www-community/attacks/xss/>
- <https://owasp.org/Top10/>
- <https://attack.mitre.org/>
- <https://cwe.mitre.org/data/definitions/79.html>
- <https://cwe.mitre.org/data/definitions/346.html>
- <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- <https://chromereleases.googleblog.com/>

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 **contacto@csirtsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.

