

Alerta ID:	125
Fecha del reporte:	17/07/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Múltiples actualizaciones de seguridad publicadas por Mozilla, Google, Adobe y VMware corrigen vulnerabilidades críticas que podrían permitir ejecución remota de código, elevación de privilegios, divulgación de información y compromiso de sistemas institucionales.
Herramienta de detección	Microsoft Defender for Endpoint, Microsoft Defender XDR, Microsoft Sentinel, Microsoft Defender Vulnerability Management, Sysmon, Windows Event Viewer, Microsoft Purview Audit, Wazuh, Splunk Enterprise Security, Elastic Security, IBM QRadar SIEM, CrowdStrike Falcon, Tenable Nessus y Qualys VMDR.
Activos involucrados:	Estaciones de trabajo y servidores que ejecuten Mozilla Firefox, Google Chrome, Adobe Acrobat Reader, Adobe Acrobat, Adobe ColdFusion, Adobe Experience Manager Forms, VMware ESXi, VMware Workstation, VMware Fusion, VMware Tools, VMware Cloud Foundation, VMware vCenter Server u otros productos VMware afectados; navegadores utilizados para el acceso a aplicaciones institucionales; servidores de virtualización; plataformas de colaboración; aplicaciones empresariales; infraestructura de usuario final; equipos administrativos; estaciones clínicas; sistemas de apoyo diagnóstico; equipos utilizados para telemedicina y cualquier activo tecnológico del sector salud que dependa de los productos incluidos en las actualizaciones de seguridad publicadas por los fabricantes.
Tipo de alerta:	Alerta
Nivel de riesgo:	Crítico

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre las actualizaciones de seguridad publicadas por **Mozilla, Google, Adobe y VMware** para corregir múltiples vulnerabilidades de alta y crítica severidad que afectan productos ampliamente utilizados en entornos empresariales y que, de ser explotadas, podrían permitir la ejecución remota de código (Remote Code Execution – RCE), elevación de privilegios, evasión de mecanismos de seguridad, divulgación de información sensible, corrupción de memoria, compromiso de máquinas virtuales y afectación de la confidencialidad, integridad y disponibilidad de los activos tecnológicos institucionales.

Las vulnerabilidades abordadas en esta alerta impactan componentes críticos de la infraestructura tecnológica, incluyendo navegadores web, soluciones de virtualización, plataformas de administración de contenidos y aplicaciones de productividad utilizadas para soportar procesos clínicos, administrativos y operacionales del sector salud. Debido a la amplia adopción de estos productos, la existencia de sistemas sin actualizar incrementa significativamente la superficie de ataque y favorece el desarrollo de campañas oportunistas y dirigidas por actores de amenaza.

La explotación exitosa de estas vulnerabilidades puede facilitar el compromiso inicial de estaciones de trabajo y servidores, el robo de credenciales, la ejecución de código arbitrario, el establecimiento de mecanismos de persistencia, el movimiento lateral dentro de la infraestructura tecnológica y el despliegue de malware, incluyendo campañas de ransomware y robo de información. En entornos hospitalarios, estos escenarios pueden afectar la continuidad de los servicios asistenciales, comprometer información clínica y administrativa, e impactar la disponibilidad de aplicaciones esenciales para la prestación de servicios de salud.

Adicionalmente, algunas de las vulnerabilidades corregidas corresponden a fallas de corrupción de memoria, uso de memoria después de liberación (*Use-After-Free*), desbordamientos de búfer, validaciones insuficientes y errores en componentes de virtualización, condiciones que históricamente han sido aprovechadas por actores de amenaza para desarrollar exploits confiables y cadenas de ataque orientadas al compromiso de infraestructuras empresariales.

El propósito de esta alerta es proporcionar a las entidades del sector salud información técnica que facilite la identificación de los productos potencialmente afectados, la priorización de las

actualizaciones de seguridad, la evaluación del nivel de exposición de los activos tecnológicos, el fortalecimiento de las capacidades de monitoreo y detección, y la implementación de medidas de mitigación y respuesta que permitan reducir el riesgo de explotación y preservar la continuidad de los servicios institucionales.

Descripción:

Mozilla, Google, Adobe y VMware publicaron recientemente actualizaciones de seguridad para corregir múltiples vulnerabilidades de alta y crítica severidad que afectan productos ampliamente utilizados en entornos empresariales, gubernamentales y del sector salud. Las fallas identificadas impactan navegadores web, plataformas de virtualización y soluciones de gestión documental y de contenidos, componentes que desempeñan un papel fundamental en la operación diaria de las organizaciones y que constituyen objetivos recurrentes para actores de amenaza debido a su amplia superficie de exposición.

Entre las vulnerabilidades corregidas se incluyen fallas de corrupción de memoria (*Memory Corruption*), uso de memoria después de su liberación (*Use-After-Free*), referencias a punteros inválidos (*Invalid Pointer Dereference*), validación insuficiente de entradas (*Improper Input Validation*), omisión de mecanismos de aislamiento (*Sandbox Escape* y *Site Isolation Bypass*), errores de gestión de privilegios y vulnerabilidades que podrían permitir la ejecución remota de código (*Remote Code Execution – RCE*), la elevación de privilegios, la divulgación de información sensible o la denegación del servicio. Este tipo de vulnerabilidades ha sido utilizado de forma reiterada por grupos de ciberdelincuencia y actores patrocinados por Estados para comprometer estaciones de trabajo, servidores e infraestructuras corporativas.

Los navegadores Mozilla Firefox y Google Chrome representan uno de los principales vectores de exposición debido a que procesan contenido procedente de Internet y son utilizados de forma permanente por usuarios administrativos, personal asistencial y contratistas para acceder a aplicaciones institucionales, servicios en la nube, plataformas gubernamentales, correo electrónico y portales clínicos. Una vulnerabilidad explotada con éxito en estos productos puede permitir que un atacante obtenga control sobre la estación de trabajo de la víctima mediante la interacción con un sitio web o contenido especialmente diseñado, facilitando el compromiso inicial de la infraestructura tecnológica.

En el caso de Adobe, las actualizaciones corrigen vulnerabilidades presentes en productos utilizados para la gestión documental, procesamiento de archivos PDF y plataformas empresariales. Dependiendo del producto afectado y de la naturaleza de la vulnerabilidad, un atacante podría ejecutar código arbitrario, evadir controles de seguridad, acceder a información restringida o comprometer servidores que soportan procesos críticos de la organización. Debido a la amplia utilización de documentos PDF en procesos administrativos, jurídicos, financieros y asistenciales, estas vulnerabilidades representan un riesgo significativo cuando las actualizaciones de seguridad no son aplicadas oportunamente.

Por su parte, VMware corrigió vulnerabilidades que afectan componentes utilizados para la virtualización y administración de infraestructuras tecnológicas. La explotación de estas fallas podría permitir el compromiso de máquinas virtuales, la afectación del hipervisor, el acceso no autorizado a sistemas virtualizados o la alteración de servicios críticos que soportan aplicaciones institucionales. En organizaciones del sector salud, donde la virtualización constituye la base de múltiples servicios clínicos y administrativos, el compromiso de estos componentes puede generar un impacto operacional considerable al afectar simultáneamente varios servicios alojados sobre una misma infraestructura física.

Las organizaciones del sector salud presentan un nivel de exposición particularmente elevado debido a la coexistencia de equipos clínicos, estaciones de trabajo administrativas, servidores de aplicaciones, plataformas de virtualización y soluciones documentales que dependen directamente de los productos incluidos en estas actualizaciones de seguridad. En este contexto, una vulnerabilidad sin corregir puede convertirse en el punto de entrada para campañas de ransomware, robo de credenciales, exfiltración de información, compromiso de sistemas de Historia Clínica Electrónica (HCE), afectación de servicios de telemedicina o interrupción de procesos asistenciales esenciales.

Considerando la criticidad de los productos afectados y la velocidad con la que los actores de amenaza incorporan nuevas vulnerabilidades a sus campañas de ataque, resulta prioritario que las entidades del sector salud identifiquen los activos potencialmente vulnerables, validen las versiones actualmente instaladas y apliquen las actualizaciones de seguridad publicadas por los fabricantes conforme a sus procedimientos de gestión de cambios y administración de vulnerabilidades. Esta medida debe complementarse con actividades de monitoreo continuo, fortalecimiento de los mecanismos de detección y revisión de posibles indicadores de compromiso que permitan identificar oportunamente intentos de explotación o compromisos previos de la infraestructura tecnológica.

Vulnerabilidades con evidencia de explotación activa

Las siguientes vulnerabilidades presentan evidencia de explotación activa, disponibilidad pública de código de explotación o un nivel de criticidad que justifica su priorización inmediata dentro de los procesos de gestión de vulnerabilidades de las entidades del sector salud.

CVE-2026-11645 – Google Chrome

- **Descripción:** Vulnerabilidad de lectura y escritura fuera de límites (Out-of-Bounds Read/Write) en el motor JavaScript V8 que puede ser explotada mediante contenido web especialmente diseñado para provocar corrupción de memoria y ejecutar código arbitrario dentro del contexto del navegador.
 - **Impacto:** Un atacante remoto podría lograr la ejecución remota de código, comprometer la estación de trabajo del usuario, instalar malware, capturar credenciales y utilizar el equipo comprometido como punto de acceso inicial hacia la infraestructura institucional.
 - **Estado de explotación:** Google confirmó que esta vulnerabilidad estaba siendo explotada activamente (Exploited in the Wild) antes de la publicación de la actualización de seguridad.
-

CVE-2026-2441 – Google Chrome

- **Descripción:** Vulnerabilidad de tipo Use-After-Free que afecta el motor JavaScript V8 y permite manipular objetos liberados en memoria mediante contenido web especialmente diseñado.
 - **Impacto:** La explotación exitosa podría permitir la ejecución remota de código, evasión de mecanismos de seguridad del navegador y compromiso de equipos utilizados para acceder a aplicaciones institucionales.
 - **Estado de explotación:** Google confirmó evidencia de explotación activa antes de la disponibilidad del parche.
-

CVE-2026-15718 – Mozilla Firefox

- **Descripción:** Vulnerabilidad de referencia inválida (Invalid Pointer) en el componente JavaScript: WebAssembly, originada por un manejo incorrecto de punteros durante el procesamiento de código WebAssembly.
 - **Impacto:** La explotación podría provocar corrupción de memoria y facilitar la ejecución de código arbitrario dentro del proceso del navegador al interactuar con contenido web especialmente diseñado.
 - **Estado de explotación:** Mozilla informó la existencia de código de explotación público (Public Exploit); sin embargo, al momento de la publicación del boletín no existe confirmación de explotación activa en entornos reales.
-

CVE-2026-15719 – Mozilla Firefox

- **Descripción:** Vulnerabilidad en el componente DOM: Navigation relacionada con los mecanismos de Site Isolation, que podría permitir eludir determinadas restricciones de aislamiento entre sitios web.
 - **Impacto:** Un atacante podría acceder a información perteneciente a otros contextos de navegación o combinar esta vulnerabilidad con otras fallas para incrementar el impacto de una cadena de explotación.
 - **Estado de explotación:** Mozilla reportó la disponibilidad de código de explotación público, sin evidencia pública de explotación activa.
-

Vulnerabilidades de Adobe

- **Descripción:** Adobe corrigió múltiples vulnerabilidades de ejecución remota de código, elevación de privilegios, corrupción de memoria, desbordamientos de búfer y divulgación de información que afectan Adobe Acrobat Reader, Adobe Acrobat, ColdFusion y Experience Manager Forms.

- **Impacto:** La explotación de estas vulnerabilidades podría permitir el compromiso de estaciones de trabajo, servidores de aplicaciones, plataformas documentales y servicios empresariales críticos utilizados por las entidades del sector salud.
 - **Estado de explotación:** Al momento de la emisión de esta alerta no existe evidencia pública de explotación activa de las vulnerabilidades corregidas en los boletines analizados.
-

Vulnerabilidades de VMware

- **Descripción:** Broadcom publicó actualizaciones para corregir múltiples vulnerabilidades que afectan VMware ESXi, VMware vCenter Server, VMware Workstation, VMware Fusion, VMware Cloud Foundation y otros componentes de virtualización, incluyendo fallas de ejecución remota de código, elevación de privilegios, divulgación de información y errores de aislamiento.
- **Impacto:** La explotación podría permitir el compromiso de hipervisores, máquinas virtuales y plataformas de administración, afectando simultáneamente múltiples servicios críticos alojados sobre la infraestructura virtualizada.
- **Estado de explotación:** Broadcom informó que algunas vulnerabilidades corregidas presentan evidencia de explotación en entornos reales, por lo que recomienda aplicar inmediatamente las actualizaciones de seguridad y verificar posibles indicadores de compromiso.

Productos y versiones afectadas

Las vulnerabilidades abordadas en esta alerta afectan múltiples productos desarrollados por Mozilla, Google, Adobe y VMware, ampliamente utilizados en estaciones de trabajo, servidores, plataformas de virtualización y aplicaciones empresariales del sector salud. La identificación oportuna de las versiones vulnerables constituye una actividad fundamental para priorizar la aplicación de las actualizaciones de seguridad, reducir la superficie de ataque y prevenir la explotación de vulnerabilidades conocidas por actores de amenaza.

Las entidades del sector salud deberán verificar las versiones actualmente instaladas en sus activos tecnológicos, contrastarlas con las versiones corregidas publicadas por los fabricantes y priorizar la actualización de aquellos sistemas que soporten servicios críticos, procesen información sensible o se encuentren expuestos a redes no confiables.

Mozilla Firefox

Las vulnerabilidades corregidas afectan las siguientes versiones del navegador:

- Mozilla Firefox anteriores a la versión 142.0.4.
- Mozilla Firefox Extended Support Release (ESR) anteriores a la versión 140.2.2 ESR.

Estas versiones corrigen, entre otras, las vulnerabilidades CVE-2026-15718 y CVE-2026-15719, relacionadas con errores de gestión de memoria y mecanismos de aislamiento del navegador.

Google Chrome

Las vulnerabilidades afectan las siguientes versiones del navegador Google Chrome:

- Windows: versiones anteriores a 139.0.7258.127/128.
- macOS: versiones anteriores a 139.0.7258.127/128.
- Linux: versiones anteriores a 139.0.7258.127.

Estas actualizaciones corrigen múltiples vulnerabilidades de alta severidad, incluyendo vulnerabilidades de tipo zero-day que fueron explotadas activamente antes de la publicación de los parches de seguridad.

Adobe

Las vulnerabilidades afectan múltiples productos empresariales de Adobe, entre ellos:

- Adobe Acrobat Reader DC anteriores a la versión 26.001.21663.
- Adobe Acrobat DC anteriores a la versión 26.001.21663.
- Adobe Acrobat 2024 anteriores a la versión 24.001.30260.
- Adobe ColdFusion 2025 anteriores a Update 3.

- Adobe ColdFusion 2023 anteriores a Update 15.
- Adobe Experience Manager (AEM) Forms 6.5 y versiones anteriores incluidas en los boletines de seguridad publicados por Adobe.

Las organizaciones que utilicen estos productos deberán validar las versiones instaladas y aplicar las actualizaciones de seguridad correspondientes, especialmente en servidores que soporten aplicaciones empresariales, plataformas de gestión documental o servicios accesibles desde Internet.

VMware

Las vulnerabilidades afectan diversos componentes de la plataforma VMware utilizados para virtualización y administración de infraestructura, incluyendo:

- VMware ESXi 8.0, incluyendo versiones anteriores a las actualizaciones de seguridad publicadas por Broadcom.
- VMware ESXi 7.0, anteriores a los parches de seguridad correspondientes.
- VMware vCenter Server 8.0, anteriores a la versión corregida publicada por Broadcom.
- VMware vCenter Server 7.0, anteriores a la actualización de seguridad correspondiente.
- VMware Workstation Pro 17.x, anteriores a la versión corregida.
- VMware Fusion 13.x, anteriores a la versión corregida.
- VMware Cloud Foundation, en las versiones afectadas identificadas por Broadcom.
- VMware Tools, en las versiones incluidas dentro de los avisos de seguridad correspondientes.

Las entidades que administren infraestructuras virtualizadas deberán verificar las versiones implementadas en hipervisores, servidores de administración y estaciones de trabajo, priorizando la actualización de aquellos sistemas que soporten servicios clínicos, plataformas de Historia Clínica Electrónica (HCE), bases de datos, servicios de autenticación, aplicaciones críticas o infraestructura expuesta a Internet.

Las organizaciones del sector salud deberán mantener un inventario actualizado de software y versiones instaladas, validar periódicamente la publicación de nuevos boletines de seguridad por parte de los fabricantes y garantizar que los activos tecnológicos permanezcan dentro de los ciclos de soporte. La identificación temprana de versiones vulnerables y la aplicación oportuna de las actualizaciones constituyen una de las medidas más efectivas para reducir el

riesgo de compromiso de la infraestructura tecnológica y preservar la continuidad de los servicios institucionales.

Consecuencias de la Explotación

La explotación exitosa de las vulnerabilidades corregidas por Mozilla, Google, Adobe y VMware puede generar afectaciones significativas sobre la confidencialidad, integridad y disponibilidad de la información, así como comprometer la infraestructura tecnológica que soporta los procesos misionales de las organizaciones del sector salud. Debido a que los productos afectados forman parte de la infraestructura de usuario final, los servicios documentales y las plataformas de virtualización, un incidente puede evolucionar rápidamente desde el compromiso de un único equipo hasta afectar múltiples activos tecnológicos de la organización.

Uno de los principales riesgos corresponde a la ejecución remota de código (Remote Code Execution – RCE), condición que permite a un actor de amenaza ejecutar instrucciones arbitrarias sobre el sistema comprometido utilizando los privilegios asociados al proceso vulnerable. Esta capacidad facilita la instalación de malware, ransomware, herramientas de administración remota (Remote Access Trojan – RAT), web shells, scripts maliciosos y otros componentes destinados a mantener el acceso persistente dentro de la infraestructura tecnológica.

Las vulnerabilidades presentes en navegadores web como Mozilla Firefox y Google Chrome incrementan el riesgo de compromiso inicial de estaciones de trabajo mediante campañas de phishing, sitios web maliciosos, publicidad comprometida (*Malvertising*) o contenido especialmente diseñado para explotar fallas del navegador. Una vez comprometido el equipo de un usuario, el atacante puede capturar credenciales, secuestrar sesiones autenticadas, instalar herramientas de acceso remoto e iniciar actividades de reconocimiento sobre la infraestructura institucional.

En el caso de los productos Adobe, la explotación puede producirse mediante la apertura de documentos PDF especialmente diseñados o mediante el compromiso de servidores que soportan aplicaciones empresariales. Esto podría permitir la alteración de documentos institucionales, el acceso no autorizado a información administrativa y clínica, la ejecución de código arbitrario sobre servidores expuestos y la interrupción de procesos relacionados con la gestión documental y los servicios digitales de la organización.

Las vulnerabilidades que afectan plataformas VMware presentan un impacto potencialmente mayor debido a que comprometen componentes centrales de la infraestructura de virtualización. Un incidente sobre el hipervisor o las plataformas de administración puede afectar simultáneamente múltiples máquinas virtuales que soportan aplicaciones críticas, bases de datos, servicios de autenticación, plataformas de Historia Clínica Electrónica (HCE), sistemas PACS, servicios de laboratorio, aplicaciones financieras y otros sistemas esenciales para la prestación de los servicios de salud.

Una vez obtenido el acceso inicial, el actor de amenaza puede desarrollar actividades de reconocimiento interno para identificar servidores críticos, controladores de dominio, recursos compartidos, plataformas de respaldo, servicios de autenticación, repositorios documentales y otros activos de alto valor. Esta información facilita el movimiento lateral, la elevación de privilegios y el compromiso progresivo de otros sistemas conectados a la infraestructura institucional.

Desde la perspectiva de la continuidad del negocio, la explotación de estas vulnerabilidades puede generar indisponibilidad parcial o total de servicios tecnológicos esenciales, afectando la atención de pacientes, la consulta de información clínica, la gestión de citas, los procesos administrativos, la facturación, la interoperabilidad entre aplicaciones y la operación de servicios asistenciales que dependen directamente de la infraestructura tecnológica.

Adicionalmente, el compromiso de equipos que procesen información personal o datos relacionados con la salud puede derivar en incidentes de seguridad con implicaciones regulatorias asociadas al tratamiento de datos personales, la confidencialidad de la información clínica y el cumplimiento de la normativa colombiana aplicable.

En términos generales, la explotación de estas vulnerabilidades podría permitir a un actor de amenaza:

- Obtener ejecución remota de código sobre estaciones de trabajo, servidores o plataformas de virtualización.
- Comprometer equipos de usuario mediante la explotación de vulnerabilidades en navegadores web o aplicaciones de escritorio.
- Instalar malware, ransomware, herramientas de acceso remoto o mecanismos de persistencia.

- Robar credenciales, cookies de autenticación, tokens de acceso e información sensible almacenada en los sistemas afectados.
- Acceder, modificar o eliminar información institucional, clínica, administrativa o financiera.
- Realizar reconocimiento de la infraestructura tecnológica e identificar activos críticos.
- Desplazarse lateralmente hacia otros sistemas corporativos mediante el uso de credenciales comprometidas.
- Interrumpir la disponibilidad de aplicaciones críticas utilizadas para soportar procesos asistenciales y administrativos.
- Facilitar campañas de espionaje, exfiltración de información, fraude o ransomware dirigidas contra organizaciones del sector salud.

Las entidades que aún no hayan aplicado las actualizaciones de seguridad publicadas por los fabricantes deben considerar estas vulnerabilidades como una prioridad alta de remediación, especialmente cuando los productos afectados se encuentren expuestos a Internet, procesen información sensible o soporten servicios esenciales para la operación institucional.

Indicadores de compromiso (IoC) y actividades de detección

La explotación de las vulnerabilidades corregidas por Mozilla, Google, Adobe y VMware puede generar diversos indicadores de compromiso que permitan identificar actividades maliciosas sobre estaciones de trabajo, servidores de aplicaciones e infraestructuras de virtualización. Debido a que los productos afectados cumplen funciones diferentes dentro de la infraestructura tecnológica, las actividades de monitoreo deben abarcar eventos del sistema operativo, registros de aplicaciones, soluciones EDR/XDR, plataformas SIEM y herramientas de administración de vulnerabilidades.

Las organizaciones del sector salud deben fortalecer temporalmente el monitoreo de estos productos hasta confirmar que la totalidad de los activos afectados han sido actualizados y que no existen evidencias de explotación previa.

Indicadores de compromiso generales

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

- Ejecución de procesos inesperados derivados de navegadores web o aplicaciones Adobe.
 - Creación de procesos hijos (*Child Processes*) desde Firefox, Chrome o Adobe Acrobat Reader.
 - Descarga y ejecución de archivos ejecutables inmediatamente después de la navegación web o la apertura de documentos PDF.
 - Creación o modificación no autorizada de tareas programadas, servicios o mecanismos de inicio automático.
 - Conexiones de red hacia direcciones IP, dominios o servicios externos no habituales para el activo comprometido.
 - Incremento inusual del consumo de CPU, memoria o actividad de disco asociado a procesos del navegador, Adobe o servicios VMware.
 - Intentos repetitivos de autenticación utilizando cuentas privilegiadas.
 - Accesos administrativos fuera del horario habitual de operación.
 - Actividades de reconocimiento interno sobre servidores, recursos compartidos o servicios de directorio.
 - Transferencias inusuales de información hacia sistemas externos.
-

Actividades de detección para Mozilla Firefox y Google Chrome

Los navegadores web constituyen uno de los principales vectores de compromiso inicial. Se recomienda monitorear:

- Procesos `firefox.exe` o `chrome.exe` generando procesos hijos como `cmd.exe`, `powershell.exe`, `wscript.exe`, `cscript.exe`, `mshta.exe`, `rundll32.exe` o `regsvr32.exe`.
- Descarga automática de archivos ejecutables desde sitios no autorizados.
- Creación de nuevas extensiones o complementos no aprobados por la organización.
- Ejecución de binarios desde directorios temporales del usuario.
- Cambios inesperados en configuraciones de seguridad del navegador.
- Incremento de alertas de Microsoft Defender SmartScreen o Safe Browsing relacionadas con navegación maliciosa.

Los equipos SOC deben correlacionar estos eventos con campañas de phishing, navegación hacia dominios recientemente registrados y alertas generadas por las soluciones EDR.

Actividades de detección para productos Adobe

En equipos que utilicen Adobe Acrobat Reader, Adobe Acrobat o productos empresariales Adobe, se recomienda revisar:

- Apertura de documentos PDF seguida de ejecución de procesos del sistema operativo.
- Ejecución de PowerShell, CMD o intérpretes de scripts inmediatamente después de abrir un documento.
- Archivos PDF provenientes de remitentes no confiables o descargados desde sitios externos.
- Intentos de conexión de aplicaciones Adobe hacia destinos externos inusuales.
- Eventos de protección generados por Microsoft Defender, EDR o antivirus asociados con documentos PDF.
- Fallos repetitivos de la aplicación que puedan indicar intentos de explotación de vulnerabilidades de corrupción de memoria.

En servidores Adobe ColdFusion o Adobe Experience Manager Forms también debe monitorearse:

- Errores de aplicación inusuales.
- Solicitudes HTTP anómalas.
- Incremento de respuestas con códigos 500.
- Ejecución inesperada de procesos desde el contexto del servicio.

Actividades de detección para VMware

Las organizaciones que administren infraestructura VMware deben incrementar el monitoreo sobre:

- Autenticaciones administrativas exitosas o fallidas desde ubicaciones no habituales.
- Creación, modificación o eliminación no autorizada de máquinas virtuales.
- Cambios inesperados en configuraciones del hipervisor o de vCenter.
- Creación de nuevas cuentas administrativas.
- Modificaciones en permisos o roles de administración.
- Transferencias masivas de máquinas virtuales o archivos VMDK.

- Eventos relacionados con elevación de privilegios o acceso a interfaces de administración.
 - Reinicios inesperados de servicios VMware.
-

Registros recomendados para revisión

Como parte de las actividades de monitoreo y detección, las organizaciones deben priorizar la revisión de los registros de eventos generados por los sistemas operativos, las aplicaciones afectadas y las plataformas de seguridad implementadas en la infraestructura tecnológica. La correlación de estos eventos permite identificar intentos de explotación, actividades posteriores al compromiso y comportamientos anómalos asociados con las vulnerabilidades abordadas en esta alerta:

- **Windows Event Viewer:** Revisar los eventos relacionados con autenticaciones exitosas y fallidas, creación de procesos, instalación o modificación de servicios, ejecución de tareas programadas, cambios en cuentas privilegiadas, modificaciones de políticas de seguridad y demás eventos registrados por el sistema operativo que puedan evidenciar actividades maliciosas.
- **Sysmon:** Analizar los eventos asociados con la creación de procesos, conexiones de red, creación o modificación de archivos, carga de bibliotecas dinámicas (DLL), cambios en el registro de Windows y ejecución de procesos desde directorios temporales o ubicaciones no habituales. Esta información resulta especialmente útil para identificar comportamientos derivados de la explotación de navegadores o aplicaciones vulnerables.
- **Microsoft Defender for Endpoint y otras soluciones EDR/XDR:** Verificar las alertas relacionadas con explotación de vulnerabilidades, ejecución de código arbitrario, comportamientos anómalos, elevación de privilegios, persistencia, movimiento lateral, ejecución de herramientas administrativas y cualquier otra actividad clasificada como de alta criticidad por la plataforma de seguridad.
- **Microsoft Sentinel o plataforma SIEM institucional:** Correlacionar eventos provenientes de estaciones de trabajo, servidores, dispositivos de red, plataformas de virtualización y soluciones de seguridad para identificar patrones de ataque, autenticaciones inusuales, conexiones hacia infraestructura externa, ejecución de

procesos sospechosos y posibles intentos de compromiso de múltiples activos tecnológicos.

- **Registros de VMware ESXi y VMware vCenter:** Revisar las autenticaciones administrativas, modificaciones de configuración, creación o eliminación de máquinas virtuales, cambios en permisos, administración de snapshots, ejecución de tareas administrativas y cualquier actividad que no corresponda con los procedimientos normales de operación de la infraestructura de virtualización.
- **Registros de Adobe ColdFusion y Adobe Experience Manager:** En los entornos que utilicen estos productos, analizar las solicitudes HTTP, errores de aplicación, excepciones, intentos de acceso no autorizado, ejecución de componentes dinámicos y demás eventos que puedan indicar actividades de reconocimiento, explotación o compromiso de los servicios.
- **Registros de servidores Proxy, Firewall y Secure Web Gateway:** Examinar las conexiones hacia dominios o direcciones IP inusuales, descargas de archivos ejecutables, transferencia de información hacia servicios externos, accesos a sitios clasificados como maliciosos y cualquier otra actividad que pueda estar asociada con la explotación de las vulnerabilidades o con la comunicación de malware con infraestructura de comando y control.

Recomendaciones para Threat Hunting

Las organizaciones que cuenten con capacidades de búsqueda proactiva de amenazas (*Threat Hunting*) deberían priorizar actividades orientadas a identificar:

- Equipos que continúen ejecutando versiones vulnerables de los productos afectados.
- Procesos hijos iniciados por navegadores web o aplicaciones PDF.
- Evidencias de explotación de vulnerabilidades mediante cadenas de ejecución inusuales.
- Persistencia basada en tareas programadas, servicios o claves de ejecución automática.
- Accesos administrativos atípicos sobre plataformas VMware.
- Equipos con conexiones recurrentes hacia infraestructura externa desconocida.
- Indicadores de movimiento lateral posteriores al compromiso inicial.
- Alertas relacionadas con explotación de vulnerabilidades clasificadas como de alta o crítica severidad.

La identificación temprana de estos comportamientos permitirá contener oportunamente posibles compromisos y reducir la probabilidad de que un incidente evolucione hacia campañas de ransomware, exfiltración de información o afectación de servicios críticos del sector salud.

Recomendaciones para administradores



Las organizaciones del sector salud que utilicen productos de Mozilla, Google, Adobe o VMware deben considerar la aplicación de las actualizaciones de seguridad como una actividad prioritaria dentro de sus procesos de gestión de vulnerabilidades. Debido a que los productos afectados forman parte de la infraestructura tecnológica que soporta procesos asistenciales, administrativos y de soporte institucional, la demora en la implementación de las correcciones incrementa la probabilidad de compromiso por parte de actores de amenaza que incorporan rápidamente las vulnerabilidades divulgadas a sus campañas de ataque.

Se recomienda realizar un inventario actualizado de todos los activos tecnológicos que ejecuten versiones de Mozilla Firefox, Google Chrome, Adobe Acrobat Reader, Adobe Acrobat, Adobe ColdFusion, Adobe Experience Manager, VMware ESXi, VMware vCenter Server, VMware Workstation y demás productos afectados, con el propósito de identificar aquellos sistemas que requieran la aplicación inmediata de las actualizaciones de seguridad.

Las entidades deben validar que las actualizaciones sean obtenidas exclusivamente desde los canales oficiales de los fabricantes y que su implementación se realice conforme a los procedimientos institucionales de gestión de cambios, garantizando previamente la disponibilidad de copias de respaldo, planes de reversión y ventanas de mantenimiento cuando se trate de servicios críticos para la operación.

En las estaciones de trabajo se recomienda verificar que los mecanismos de actualización automática de Mozilla Firefox y Google Chrome permanezcan habilitados, evitando que los usuarios operen versiones obsoletas de los navegadores. Asimismo, deben eliminarse aquellas versiones que hayan alcanzado el fin de su ciclo de soporte o que ya no reciban actualizaciones de seguridad por parte del fabricante.

En los equipos que utilicen Adobe Acrobat Reader o Adobe Acrobat, es recomendable mantener habilitados los mecanismos de protección nativos de la plataforma, incluyendo **Protected Mode**, **Protected View** y las restricciones para la ejecución de contenido activo

cuando estas funcionalidades sean compatibles con los procesos institucionales. Adicionalmente, debe restringirse la apertura de documentos PDF provenientes de fuentes no confiables y fortalecer los controles de seguridad asociados al correo electrónico institucional.

Para los entornos que utilicen Adobe ColdFusion, Adobe Experience Manager u otras soluciones empresariales de Adobe, se recomienda limitar la exposición de los servicios a Internet, implementar controles de autenticación robusta para las interfaces administrativas, restringir el acceso mediante listas de control, segmentar la infraestructura donde sea técnicamente viable y revisar periódicamente la configuración de seguridad de las aplicaciones.

En las plataformas VMware resulta prioritario restringir el acceso a las interfaces de administración únicamente al personal autorizado, implementar autenticación multifactor (MFA) cuando esté disponible, revisar periódicamente las cuentas con privilegios administrativos, eliminar credenciales obsoletas y verificar que los servicios de administración no permanezcan expuestos directamente a Internet salvo que exista una necesidad operacional debidamente justificada y protegida mediante controles compensatorios.

Las organizaciones también deben fortalecer sus procesos de gestión de vulnerabilidades mediante la ejecución periódica de análisis de seguridad que permitan identificar versiones desactualizadas, configuraciones inseguras y componentes que hayan alcanzado el fin de soporte del fabricante. Los resultados obtenidos deben integrarse con los planes institucionales de remediación y priorizarse de acuerdo con el nivel de criticidad de los activos y el impacto potencial sobre la prestación de los servicios de salud.

Se recomienda verificar que las soluciones EDR/XDR, antivirus, plataformas SIEM y herramientas de administración de vulnerabilidades se encuentren correctamente actualizadas y configuradas para detectar intentos de explotación relacionados con las vulnerabilidades corregidas. De igual forma, las reglas de correlación y los casos de uso del SOC deben actualizarse para incorporar los nuevos escenarios de riesgo asociados con los productos afectados.

Finalmente, las entidades deben promover campañas permanentes de sensibilización dirigidas a usuarios finales, administradores de sistemas y personal de soporte, orientadas a reforzar las buenas prácticas de navegación segura, el manejo adecuado de documentos electrónicos, la identificación de intentos de phishing y la importancia de mantener actualizados los equipos

institucionales como una medida fundamental para reducir la superficie de ataque y fortalecer la postura de ciberseguridad de la organización.

Medidas de mitigación inmediatas

Mientras las actualizaciones de seguridad son evaluadas, probadas e implementadas conforme a los procedimientos institucionales de gestión de cambios, las organizaciones del sector salud deben adoptar medidas de mitigación orientadas a reducir la superficie de ataque y disminuir la probabilidad de explotación de las vulnerabilidades abordadas en esta alerta.

Como primera medida, se recomienda identificar todos los activos tecnológicos que ejecuten versiones vulnerables de Mozilla Firefox, Google Chrome, Adobe Acrobat Reader, Adobe Acrobat, Adobe ColdFusion, Adobe Experience Manager, VMware ESXi, VMware vCenter Server y demás productos afectados, estableciendo un inventario actualizado que permita priorizar la aplicación de las correcciones de acuerdo con la criticidad de cada activo y el impacto sobre los procesos institucionales.

Las organizaciones deben verificar que las actualizaciones de seguridad publicadas por los fabricantes se encuentren disponibles para su despliegue y priorizar su instalación en aquellos sistemas expuestos a Internet, plataformas que procesen información sensible, servidores de virtualización, aplicaciones críticas para la prestación de servicios de salud y estaciones de trabajo utilizadas por personal con privilegios elevados.

Cuando la actualización inmediata no sea posible por restricciones operativas o requerimientos de continuidad del negocio, deberán implementarse controles compensatorios que reduzcan el nivel de exposición. Entre ellos se incluyen la restricción del acceso a interfaces administrativas, el fortalecimiento de los controles de autenticación, la limitación de servicios accesibles desde redes externas, la segmentación de los sistemas afectados y el incremento del monitoreo sobre los activos vulnerables hasta completar el proceso de actualización.

En los navegadores Mozilla Firefox y Google Chrome se recomienda deshabilitar o eliminar extensiones que no sean estrictamente necesarias para la operación institucional, restringir la instalación de nuevos complementos por parte de los usuarios, mantener habilitados los mecanismos de navegación segura proporcionados por los fabricantes y aplicar las políticas corporativas de seguridad mediante las herramientas centralizadas de administración de dispositivos.

En los equipos que utilicen Adobe Acrobat Reader o Adobe Acrobat debe reforzarse el control sobre la apertura de archivos PDF provenientes de fuentes externas o remitentes desconocidos, especialmente cuando estos sean recibidos por correo electrónico o descargados desde Internet. Asimismo, se recomienda mantener habilitadas las funcionalidades de aislamiento y protección incorporadas por el fabricante, reduciendo el riesgo de ejecución de contenido potencialmente malicioso.

Para las plataformas Adobe ColdFusion, Adobe Experience Manager y demás soluciones empresariales, se recomienda restringir el acceso a las consolas administrativas mediante listas de control de acceso, redes privadas virtuales (VPN) o mecanismos equivalentes, evitando su exposición directa a Internet mientras se completan las actividades de actualización y validación.

En los entornos VMware, las organizaciones deben revisar las cuentas administrativas existentes, validar que únicamente el personal autorizado conserve privilegios elevados, restringir el acceso remoto a las interfaces de administración, verificar la integridad de las configuraciones del hipervisor y revisar los registros de auditoría en busca de actividades administrativas inusuales o modificaciones no autorizadas.

Como medida adicional de reducción del riesgo, se recomienda ejecutar análisis de vulnerabilidades sobre los activos identificados para confirmar el estado de actualización de los productos afectados y verificar que las correcciones hayan sido aplicadas correctamente. Los resultados obtenidos deben documentarse y utilizarse para actualizar el inventario institucional de vulnerabilidades.

Finalmente, hasta confirmar la remediación completa de los activos afectados, las organizaciones deben incrementar la frecuencia del monitoreo de eventos de seguridad, fortalecer las actividades de *Threat Hunting*, revisar continuamente las alertas generadas por las soluciones EDR/XDR y SIEM, y mantener comunicación permanente entre los equipos de infraestructura, ciberseguridad y respuesta a incidentes para facilitar la detección temprana de cualquier intento de explotación asociado con las vulnerabilidades descritas en esta alerta.

Acciones de respuesta ante un posible compromiso

Si una organización identifica evidencias de explotación o indicadores que sugieran el compromiso de alguno de los productos abordados en esta alerta, deberá activar inmediatamente su procedimiento institucional de gestión de incidentes de seguridad de la información, con el propósito de contener el incidente, preservar las evidencias digitales, determinar el alcance de la afectación y restablecer las condiciones normales de operación de los servicios tecnológicos.

Como primera acción, se recomienda identificar los equipos, servidores o plataformas potencialmente comprometidos y evaluar si continúan representando un riesgo para la infraestructura institucional. Cuando existan evidencias razonables de explotación, los activos afectados deberán aislarse de la red de forma controlada para evitar la propagación del incidente, sin interrumpir innecesariamente los procesos de adquisición de evidencias o las actividades de análisis forense.

Durante la fase inicial de respuesta, es fundamental preservar la evidencia digital asociada al incidente. Las organizaciones deben recopilar registros de eventos, archivos de auditoría, capturas de memoria, conexiones de red activas, procesos en ejecución, registros de autenticación y cualquier otro elemento que permita reconstruir la secuencia de los hechos e identificar las técnicas utilizadas por el actor de amenaza. La recolección de evidencias debe realizarse siguiendo los procedimientos institucionales establecidos para garantizar su integridad y trazabilidad.

Una vez contenido el incidente, debe determinarse el alcance del compromiso mediante actividades de análisis técnico orientadas a identificar otros activos afectados, cuentas comprometidas, mecanismos de persistencia, herramientas maliciosas instaladas, movimientos laterales y posibles actividades de exfiltración de información. Esta evaluación debe extenderse a los sistemas que mantengan relaciones de confianza con los equipos comprometidos, especialmente cuando se trate de plataformas de virtualización o servidores que soporten servicios críticos.

Si durante la investigación se identifica el compromiso de credenciales de usuario o cuentas con privilegios elevados, deberán ejecutarse de forma inmediata los procedimientos de restablecimiento de credenciales, revocación de sesiones activas, rotación de claves de servicio

y revisión de los permisos asignados, priorizando las cuentas administrativas y aquellas utilizadas para la administración de infraestructura tecnológica.

En los entornos VMware, además de las actividades anteriores, se recomienda revisar detalladamente las acciones administrativas ejecutadas sobre el hipervisor y las plataformas de gestión, validar la integridad de las máquinas virtuales, verificar que no existan cambios no autorizados en la configuración del entorno y confirmar que las copias de seguridad permanezcan disponibles e íntegras antes de iniciar cualquier proceso de recuperación.

Cuando el incidente involucre estaciones de trabajo afectadas por la explotación de vulnerabilidades en navegadores web o productos Adobe, deberá verificarse la existencia de malware, herramientas de acceso remoto, mecanismos de persistencia, tareas programadas, servicios no autorizados y modificaciones en la configuración del sistema operativo que puedan facilitar un nuevo compromiso una vez el equipo sea reincorporado a la red.

Antes de restablecer los servicios afectados, la organización debe confirmar que las vulnerabilidades hayan sido corregidas mediante la instalación de las actualizaciones publicadas por los fabricantes, verificar que no existan indicadores de compromiso activos y ejecutar actividades de validación técnica que permitan confirmar el adecuado funcionamiento de los controles de seguridad implementados.

Finalmente, una vez concluido el proceso de recuperación, se recomienda documentar las lecciones aprendidas, actualizar los procedimientos de respuesta a incidentes, incorporar los nuevos indicadores de detección a las plataformas de monitoreo y fortalecer las capacidades institucionales de prevención, detección y respuesta frente a futuras campañas que aprovechen vulnerabilidades similares.

Mapeo con MITRE ATT&CK

Las vulnerabilidades corregidas por Mozilla, Google, Adobe y VMware pueden ser incorporadas por actores de amenaza dentro de diferentes fases de una cadena de ataque.

Dependiendo del producto afectado, del nivel de acceso obtenido y de los objetivos del atacante, la explotación puede facilitar el compromiso inicial de estaciones de trabajo, servidores de aplicaciones o infraestructuras de virtualización, permitiendo posteriormente el

establecimiento de persistencia, la elevación de privilegios, el movimiento lateral y la exfiltración de información.

El siguiente mapeo presenta las principales tácticas y técnicas del marco **MITRE ATT&CK** que podrían observarse durante la explotación de las vulnerabilidades abordadas en esta alerta:

- **T1190 – Exploit Public-Facing Application:** Puede presentarse cuando un actor de amenaza explota vulnerabilidades presentes en servidores Adobe ColdFusion, Adobe Experience Manager o componentes VMware expuestos a Internet, obteniendo acceso inicial a la infraestructura tecnológica.
- **T1189 – Drive-by Compromise:** Aplica a escenarios donde un usuario accede a un sitio web especialmente diseñado para explotar vulnerabilidades presentes en Mozilla Firefox o Google Chrome sin requerir la descarga consciente de archivos maliciosos.
- **T1059 – Command and Scripting Interpreter:** Una vez explotada la vulnerabilidad, el atacante puede ejecutar comandos mediante PowerShell, CMD, Bash u otros intérpretes disponibles en el sistema comprometido para descargar herramientas adicionales, modificar configuraciones o iniciar actividades de reconocimiento.
- **T1547 – Boot or Logon Autostart Execution:** Los actores de amenaza pueden establecer mecanismos de persistencia mediante tareas programadas, claves de ejecución automática, servicios del sistema o modificaciones en la configuración del sistema operativo.
- **T1505 – Server Software Component:** En servidores comprometidos, particularmente aquellos que ejecutan Adobe ColdFusion o servicios empresariales, el atacante puede instalar componentes maliciosos que le permitan mantener acceso persistente al entorno.
- **T1068 – Exploitation for Privilege Escalation:** Algunas vulnerabilidades pueden ser utilizadas para obtener privilegios superiores sobre el sistema comprometido, facilitando el acceso a recursos restringidos o la administración completa del equipo.

- **TA0006 – Credential Access (Acceso a Credenciales):** Una vez comprometido el activo, el atacante puede intentar obtener credenciales almacenadas en memoria o en el sistema operativo para ampliar el alcance del incidente.
- **T1555 – Credentials from Password Stores:** También pueden buscarse credenciales almacenadas por navegadores web o aplicaciones utilizadas por los usuarios institucionales.
- **T1082 – System Information Discovery:** Permite recopilar información del sistema operativo, versiones instaladas y configuración del equipo comprometido.
- **T1018 – Remote System Discovery:** Utilizada para identificar otros equipos conectados a la infraestructura institucional y planificar movimientos laterales.
- **T1087 – Account Discovery:** Orientada a identificar usuarios locales, cuentas de dominio y grupos con privilegios elevados.
- **T1021 – Remote Services:** Las credenciales obtenidas durante el compromiso inicial pueden utilizarse para acceder a otros servidores mediante protocolos administrativos como RDP, SMB, WinRM o SSH, ampliando progresivamente el alcance del incidente.
- **T1041 – Exfiltration Over C2 Channel:** La información obtenida puede ser transferida hacia la infraestructura controlada por el atacante utilizando los mismos canales de comunicación empleados para el comando y control.
- **T1567 – Exfiltration Over Web Service:** También puede emplearse el uso de servicios web o almacenamiento en la nube para extraer documentos, bases de datos y otra información institucional sin generar tráfico inusual.

Fuentes:

- <https://thehackernews.com/2026/07/firefox-chrome-adobe-and-vmware-updates.html>
- <https://www.mozilla.org/en-US/security/advisories/>
- <https://www.mozilla.org/en-US/firefox/releases/>
- <https://chromereleases.googleblog.com/>
- <https://chromium.googlesource.com/chromium/src/+main/docs/security/>

- <https://helpx.adobe.com/security.html>
- <https://helpx.adobe.com/security/security-bulletin.html>
- <https://support.broadcom.com/web/ecx/security-advisories>
- <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- <https://www.cisa.gov/news-events/cybersecurity-advisories>
- <https://attack.mitre.org/>
- <https://www.cve.org/>
- <https://nvd.nist.gov/>

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.