

|                          |                                                                                             |
|--------------------------|---------------------------------------------------------------------------------------------|
| Alerta ID:               | 123                                                                                         |
| Fecha del reporte:       | 08/07/2026                                                                                  |
| Entidad:                 | Todas las entidades del ecosistema digital                                                  |
| Título:                  | Alerta de Vulnerabilidad Crítica con Explotación Activa - Adobe ColdFusion – CVE-2026-48282 |
| Herramienta de detección | N/A                                                                                         |
| Activo involucrado:      | Adobe ColdFusion                                                                            |
| Tipo de alerta:          | Alerta                                                                                      |
| Nivel de riesgo:         | Alto                                                                                        |

**Objetivo:**

Informar a las organizaciones del sector salud en Colombia sobre la identificación de la vulnerabilidad crítica **CVE-2026-48282**, que afecta al producto **Adobe ColdFusion** y que podría permitir la ejecución de código arbitrario en servidores donde se encuentren implementadas versiones vulnerables de la plataforma. Esta falla de seguridad puede comprometer la confidencialidad, integridad y disponibilidad de la información almacenada o procesada por aplicaciones desarrolladas sobre ColdFusion, afectando servicios tecnológicos utilizados para soportar procesos clínicos, administrativos y operativos dentro de las instituciones de salud.



El propósito de esta alerta es que las organizaciones del sector salud validen si utilizan **Adobe ColdFusion** dentro de su infraestructura tecnológica, ya sea en servidores propios, ambientes virtualizados, servicios en la nube, plataformas administradas por terceros o aplicaciones desarrolladas internamente. Esta validación debe incluir la revisión del inventario tecnológico, identificación de versiones instaladas, servidores expuestos a internet, aplicaciones web asociadas, integraciones con sistemas institucionales y cualquier componente que pueda procesar información crítica relacionada con pacientes, procesos administrativos o servicios misionales.

#### Descripción:

Adobe ha publicado actualizaciones de seguridad para corregir la vulnerabilidad identificada como **CVE-2026-48282**, que afecta a **Adobe ColdFusion 2025 y Adobe ColdFusion 2023**. Esta vulnerabilidad corresponde a una condición de **Path Traversal (CWE-22)** ocasionada por una validación insuficiente de rutas y accesos a recursos dentro de la aplicación, permitiendo que un atacante pueda manipular solicitudes especialmente diseñadas para acceder a ubicaciones no autorizadas dentro del servidor afectado.

La explotación de esta vulnerabilidad podría permitir a un atacante remoto acceder a archivos restringidos, modificar componentes del sistema o ejecutar código arbitrario en el contexto del servicio ColdFusion. Esta condición representa un riesgo crítico debido a que los servidores ColdFusion suelen alojar aplicaciones web institucionales, sistemas administrativos, portales internos y soluciones integradas con procesos organizacionales.

El fallo se presenta cuando el servidor procesa solicitudes manipuladas que contienen rutas diseñadas para evadir los controles normales de acceso. Un atacante podría aprovechar esta



debilidad sin requerir privilegios administrativos iniciales, utilizando únicamente comunicación con el servicio vulnerable expuesto en la red.

Esta vulnerabilidad adquiere especial relevancia para el sector salud debido a que un compromiso exitoso del servidor podría afectar aplicaciones que gestionan información clínica, datos administrativos, reportes institucionales, integraciones con sistemas hospitalarios y plataformas utilizadas por usuarios internos o externos.

Adobe ha publicado actualizaciones de seguridad que corrigen la vulnerabilidad fortaleciendo los mecanismos de validación de rutas, control de acceso y procesamiento seguro de solicitudes. Se recomienda aplicar las actualizaciones inmediatamente, debido a que la vulnerabilidad cuenta con reportes de explotación activa y podría generar impactos graves sobre la seguridad y continuidad operacional de las organizaciones de salud.

### Consecuencias de la explotación

La explotación exitosa de la vulnerabilidad **CVE-2026-48282** en Adobe ColdFusion puede generar consecuencias críticas a nivel técnico, operativo y de seguridad de la información para las organizaciones del sector salud. Debido a que ColdFusion suele utilizarse como plataforma para aplicaciones web institucionales, un compromiso podría afectar servidores que soportan procesos esenciales. Entre las principales consecuencias se destacan:

#### 1. Ejecución de código arbitrario en servidores institucionales:

Los atacantes podrían aprovechar la vulnerabilidad para ejecutar instrucciones no autorizadas dentro del servidor donde opera Adobe ColdFusion, permitiendo modificar archivos, instalar componentes maliciosos o alterar el funcionamiento normal de las aplicaciones alojadas.



**2. Acceso no autorizado a información sensible:**

Un servidor comprometido podría permitir el acceso a información almacenada o procesada por las aplicaciones ColdFusion, incluyendo datos administrativos, información personal, configuraciones internas, credenciales o información relacionada con procesos clínicos.

**3. Compromiso de aplicaciones web institucionales:**

La explotación podría afectar portales, aplicativos internos, sistemas de gestión, plataformas de reportes o herramientas desarrolladas sobre ColdFusion, generando alteración de funcionalidades, indisponibilidad o manipulación de información.

**4. Movimiento lateral dentro de la infraestructura tecnológica:**

Un atacante que comprometa un servidor ColdFusion podría utilizarlo como punto inicial para realizar reconocimiento interno, acceder a otros sistemas conectados, comprometer bases de datos, servidores administrativos o plataformas críticas de la organización.

**5. Interrupción de servicios esenciales:**

La modificación o afectación del servidor podría generar indisponibilidad de aplicaciones utilizadas por áreas asistenciales y administrativas, impactando procesos como consulta de información, generación de reportes, gestión documental o servicios internos.

**6. Riesgos reputacionales:**

La exposición de información sensible o la interrupción de servicios tecnológicos podría afectar la confianza de pacientes, colaboradores, proveedores y entidades reguladoras.

**7. Impacto regulatorio y cumplimiento normativo:**

La exposición de datos personales o información sensible derivada de un incidente podría generar investigaciones o sanciones relacionadas con la protección de datos personales, conforme a la **Ley 1581 de 2012** en Colombia y demás regulaciones aplicables.

### Modo de explotación del ataque

La explotación de la vulnerabilidad **CVE-2026-48282** en Adobe ColdFusion puede desarrollarse mediante las siguientes fases:

#### **Fase 1 – Identificación de servidores ColdFusion vulnerables**

El atacante inicia realizando actividades de reconocimiento para identificar servidores que ejecutan Adobe ColdFusion y determinar versiones vulnerables. Esto puede realizarse mediante análisis de servicios publicados, búsqueda de aplicaciones web expuestas o identificación de tecnologías utilizadas por la organización.

#### **Fase 2 – Envío de solicitudes manipuladas**

Una vez identificado un servidor vulnerable, el atacante envía solicitudes especialmente diseñadas utilizando técnicas de manipulación de rutas (*Path Traversal*) con el objetivo de evadir los mecanismos de restricción establecidos por la aplicación.

#### **Fase 3 – Acceso no autorizado y ejecución de código**

Al explotar la vulnerabilidad, el atacante puede acceder a recursos restringidos del servidor o ejecutar código dentro del contexto del servicio ColdFusion, obteniendo capacidad para modificar archivos, alterar aplicaciones o ejecutar acciones no autorizadas.

#### **Fase 4 – Compromiso de información y aplicaciones**



Con acceso al servidor, el atacante podría consultar información sensible, extraer datos, modificar aplicaciones alojadas o acceder a configuraciones internas que permitan ampliar el alcance del ataque.

#### **Fase 5 – Persistencia y movimiento lateral**

El atacante podría establecer mecanismos de persistencia, crear accesos adicionales, modificar configuraciones o utilizar el servidor comprometido para desplazarse hacia otros sistemas internos de la organización.

#### **Vulnerabilidades asociadas**

- La vulnerabilidad **CVE-2026-48282** se origina por debilidades propias en los mecanismos de validación y control de rutas utilizados por Adobe ColdFusion, permitiendo que solicitudes manipuladas puedan acceder a recursos fuera del alcance autorizado.
- **Fallas en la validación de rutas de acceso:** La vulnerabilidad permite que un atacante manipule rutas dentro de solicitudes web para acceder a archivos o directorios restringidos del servidor, comprometiendo la seguridad del sistema.
- **Procesamiento inseguro de solicitudes externas:** La falta de validaciones adecuadas sobre entradas proporcionadas por usuarios externos incrementa el riesgo de explotación mediante solicitudes diseñadas específicamente para evadir controles.



- **Exposición de información sensible del servidor:** La explotación puede permitir acceso a archivos de configuración, credenciales, componentes internos o información utilizada por aplicaciones institucionales.
- **Configuraciones inseguras del servidor:** Instalaciones con configuraciones predeterminadas, permisos excesivos o exposición directa a internet aumentan la probabilidad de compromiso.
- **Falta de controles complementarios:** La ausencia de segmentación, monitoreo, controles de acceso y políticas de mínimo privilegio puede incrementar el impacto de una explotación exitosa.

### Recomendaciones de detección y mitigación



Los equipos de seguridad, infraestructura y administración de TI deben priorizar la identificación y actualización inmediata de todas las instalaciones de **Adobe ColdFusion** afectadas.

Se recomienda:

1. **Actualizar Adobe ColdFusion inmediatamente:**
2. Aplicar los parches publicados por Adobe:
  - ColdFusion 2025 Update 10.



- ColdFusion 2023 Update 21.

Validar servidores productivos, pruebas, contingencia y ambientes administrados por terceros.

## **2. Realizar inventario tecnológico:**

Identificar servidores ColdFusion, aplicaciones asociadas, versiones instaladas, responsables técnicos y exposición hacia internet.

## **3. Revisar registros del servidor:**

Monitorear:

- Solicitudes HTTP anómalas.
- Intentos de acceso a rutas restringidas.
- Errores inesperados del servicio.
- Creación o modificación de archivos.
- Ejecución de procesos desconocidos.

## **4. Restringir exposición externa:**

Limitar accesos públicos únicamente a servicios necesarios mediante firewall, listas de control y segmentación de red.



**5. Revisar permisos del servidor:**

Aplicar mínimo privilegio sobre usuarios y servicios que ejecutan ColdFusion.

**6. Realizar análisis de compromiso:**

En servidores expuestos, revisar indicadores de compromiso antes y después de aplicar actualizaciones.

**Recomendaciones de prevención y mitigación****1. Aplicar actualizaciones de seguridad inmediatamente:**

2. Actualizar todas las instalaciones vulnerables de Adobe ColdFusion a versiones soportadas y corregidas.

**2. Implementar controles de acceso estrictos:**

Aplicar segmentación de red, restricciones administrativas y políticas de mínimo privilegio.

**3. Fortalecer servidores web y aplicaciones:**

Configurar reglas de firewall, WAF y controles de filtrado para bloquear solicitudes sospechosas.

**4. Proteger credenciales institucionales:**

Evitar almacenamiento inseguro de credenciales y realizar rotación periódica de accesos críticos.

**5. Implementar monitoreo continuo:**

Integrar registros de ColdFusion, servidores y aplicaciones con herramientas SIEM.

**6. Realizar evaluaciones periódicas de vulnerabilidades:**

Ejecutar análisis de seguridad sobre aplicaciones web y servidores institucionales.

**7. Aplicar defensa en profundidad:**

Mantener antivirus/EDR, firewall, segmentación, respaldo seguro y controles de seguridad complementarios.

**Recomendaciones de respuesta ante compromiso**

En caso de confirmar explotación de **CVE-2026-48282**, se recomienda:

- 1. Aislar inmediatamente el servidor afectado:**
2. Restringir conexiones para evitar propagación o actividad adicional del atacante.

**2. Aplicar actualizaciones de seguridad:**

Actualizar Adobe ColdFusion a versiones corregidas.



**3. Preservar evidencias:**

Recolectar logs, configuraciones, archivos modificados y registros de actividad.

**4. Revisar accesos y credenciales:**

Cambiar credenciales administrativas y aquellas utilizadas por aplicaciones comprometidas.

**5. Analizar posibles movimientos laterales:**

Revisar conexiones hacia bases de datos, servidores internos y aplicaciones relacionadas.

**6. Realizar análisis forense:**

Determinar alcance, método de acceso y acciones realizadas por el atacante.

**7. Restaurar desde copias seguras:**

Recuperar sistemas desde respaldos verificados cuando exista manipulación o compromiso.

**8. Reportar el incidente:**

Informar al CSIRT interno, responsables de seguridad y autoridades correspondientes cuando aplique.

**9. Fortalecer controles posteriores:**

Implementar mejoras derivadas del análisis de causa raíz.

### Conclusiones

La vulnerabilidad **CVE-2026-48282** representa un riesgo crítico para las organizaciones del sector salud que utilizan **Adobe ColdFusion** como plataforma para aplicaciones web institucionales. Su explotación podría permitir la ejecución de código arbitrario en servidores afectados, comprometiendo información sensible, aplicaciones misionales y servicios tecnológicos utilizados para soportar procesos clínicos y administrativos.

El impacto de esta vulnerabilidad puede extenderse desde la afectación técnica de servidores y aplicaciones hasta consecuencias operativas relacionadas con disponibilidad de servicios, protección de datos de pacientes y continuidad institucional.

La aplicación inmediata de las actualizaciones de seguridad, junto con controles de monitoreo, segmentación, revisión de configuraciones y fortalecimiento de políticas de seguridad, es fundamental para reducir el riesgo de explotación.

Las organizaciones del sector salud deben mantener una gestión continua de vulnerabilidades, asegurando que sus servidores y aplicaciones permanezcan actualizados, protegidos y alineados con buenas prácticas de ciberseguridad.

La adopción de estas medidas permitirá fortalecer la protección de la información clínica y administrativa, garantizar la continuidad de los servicios tecnológicos y reducir la exposición frente a amenazas emergentes.

### Fuentes:



- 
- Adobe Security Bulletin – ColdFusion Security Updates  
Información oficial del fabricante sobre vulnerabilidades, versiones afectadas y actualizaciones disponibles.

o URL: <https://helpx.adobe.com/security/products/coldfusion.html>

- National Vulnerability Database (NVD) – CVE-2026-48282  
Información técnica, clasificación CVSS, descripción y referencias de la vulnerabilidad.

o URL: <https://nvd.nist.gov/>

- MITRE CVE Database – CVE-2026-48282  
Registro oficial de la vulnerabilidad y referencias asociadas.

o URL: <https://cve.mitre.org/>

- NHS England Digital – Cyber Alert Adobe ColdFusion CVE-2026-48282  
Alerta técnica para sector salud sobre explotación activa y recomendaciones.

o URL: <https://digital.nhs.uk/cyber-alerts>

- CISA Known Exploited Vulnerabilities Catalog  
Catálogo de vulnerabilidades explotadas activamente.

o URL: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

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.

